Information Security Policy

Document Title	Information Security Policy - Public
Document ID	MM-ISMS-PL-01
Owner	Marcel Lehner (CISO)
Approver(s)	Peter Oswald (CEO), Franz Hiesinger (CFO), Jacqueline Wild (Head of Group IM)
Contact for advice	Group Security security@mm.group
Effective Date	01.02.2018
Last Updated	01.07.2022

1 Mission Statement

Mayr-Melnhof Karton AG / MM Group (MM) is the world's top manufacturer of coated recycled cardboard and the premier provider of folding cartons in Europe. Our main objective is to foster sustainable development by offering innovative, eco-friendly packaging and paper solutions. We utilise cutting-edge information and communication technology devices and processes to accomplish this, ensuring efficient, high-quality, and timely internal operations and customer deliveries.

Recognising the critical importance of secure and consistently available information processing, we prioritise information security at MM. This is because technical glitches, misconduct, sabotage, and espionage can significantly threaten the functionality and availability of our IT systems and networks and the confidentiality and integrity of our business processes and data. In severe cases, this could damage our reputation, causing financial losses and potential environmental and human risks.

To mitigate these risks, we have established an integrated information security management system (ISMS) that effectively safeguards confidentiality, availability, integrity, and authenticity sustainably and cost-effectively.

1.1 Information Security Culture

At MM, we highly value the trust of our customers when it comes to the quality and security of our services. This encompasses safeguarding data and information essential for the smooth operation of our offices and production facilities and any customer-generated data processed individually.

We take all necessary and economically feasible measures according to the latest technologies to ensure the safety and protection of our services, facilities, data, and information.

Our commitment to information security is an integral part of MM's corporate culture, which guides our perception, thinking, and actions related to information security. It is deeply ingrained in our company's informal structures and is exemplified through the actions of our executive team, who strive to instil this culture in all of our employees.

1.2 Objectives of Information Security

At MM, we prioritise information security. Our objectives include the following:

- Employing state-of-the-art methods to secure our services, facilities, data, and information prevents unauthorised access or theft.
- Diligently complying with legal requirements for information security and data protection, as required by law, in a timely and comprehensive manner.
- Evaluating the risks posed by new technologies and incorporating information security into our decision-making process for procurement and operation, emphasising efficiency and ease of use.
- Continuously improving and updating our security measures to adapt to the evolving threat landscape, ensuring we stay ahead of potential risks and vulnerabilities.
- Providing regular training and awareness programs for our employees to promote a security-conscious mindset and empower them to recognise and prevent potential security incidents.
- Establishing a transparent and efficient incident response plan to swiftly identify, contain, and remediate any security breaches, thereby minimising their impact and preventing future occurrences.

By embracing these goals, we strive to foster a robust security culture and guarantee our data protection.

1.3 Information Security Strategy

Our objectives have been achieved through the implementation of the following points:

- An information security management system (ISMS) has been established based on internationally recognised standards.
- An information security risk management system (IS-RM) has been implemented to provide management with the information needed to make informed decisions regarding information security risks.
- Our team has established a training and awareness program to keep all employees up-to-date with the latest technical knowledge and information security best practices.
- Key performance indicators (KPIs) and audit measures have been established to continually evaluate and improve the effectiveness and quality of our ISMS and operational measures.
- We have established processes for legally required communication with authorities and customers in case of any security incidents or inquiries related to personal data and information.

2 Scope, Integration within the company

Our Information Security Policy applies to MM and all its subsidiaries, regardless of location. It covers everything we do, including processes, assets, and information, all of which are important for achieving our corporate objectives. We require all contractors to know and follow this policy, especially when buying new IT systems. We ensure this by including the relevant regulation in our purchasing conditions and planning documents. We may also use this policy as a reference when creating individual contracts. All our employees must follow the principles and standards outlined below when dealing with information assets. This includes planning, developing, procuring, setting up, operating, and disposing of them.

3 Principles

Our information security management system is designed and continually improved according to ISO/IEC 27001:2022 and other well-known standards and frameworks, with the following key principles in mind:

- Corporate policies and organisational instructions guide the design of each principle.
- Information security objectives are aligned with MM's overall goals, promoting a culture of security awareness and commitment throughout the company.
- Information security measures and risk management processes are derived from our information security policy.
- We use basic protection measures and detailed risk analysis to achieve a risk-adaptive security level.
- We select and implement information security measures based on the level of risk, considering state of the art, which we periodically review and update as part of our ongoing innovation process.
- Employees receive only the information necessary for their duties, with technical or organisational measures preventing information overload. We separate incompatible functions, roles, and responsibilities to avoid errors and manipulation. If functional separation is not feasible, we implement approved compensating measures.
- Following our information security policy, we maintain a log of all information access and ensure that it is carried out solely within the scope of assigned tasks.
- Internal and external audits and regular risk analyses evaluate compliance with principles and the effectiveness of our information security management system. We document results and develop specific measures accordingly.
- Data and information are classified based on confidentiality, integrity, availability, and data protection relevance.
- We regularly provide employees with training and awareness initiatives to promote responsible information handling.
- The information security management system (ISMS) requirements are directly applied to new IT systems. For existing systems, a separate transfer agreement was made.
- We maintain an adequate performance measurement system to continuously improve our information security management system.
- Incident management processes are in place to identify, assess, and respond to security incidents, ensuring timely communication and resolution.
- Third-party vendors and partners are carefully evaluated to ensure they meet our information security standards and maintain the same level of commitment to data protection.
- Business continuity and disaster recovery plans are developed, tested, and updated regularly to minimize the impact of potential disruptions and ensure the quick restoration of operations.
- Continuous monitoring and improvement of our information security management system is achieved through the collection and analysis of relevant metrics, which inform decision-making and help us identify areas for enhancement.

4 Enforcement and Sanctioning

The management teams are in charge of making sure that proper information security measures are put into place. We actively monitor adherence to these security measures. If employees are not following them, the management teams will guide them on their responsibilities. If needed, any violations will be appropriately addressed.

5 Declaration of Binding Commitment

MM's leadership and IT management established an information security policy, version 2.0, effective July 1, 2022. This policy is the foundation for all IT-related decisions and actions within the company. It aligns with our broader corporate strategies and is crucial in achieving our business objectives and executing our IT strategy. MM is dedicated to implementing, maintaining, and continually enhancing this information security policy.

Starting from July 1, 2022, the information security policy, associated standards, guidelines and work instructions will be mandatory for all MM employees, including those at majority-owned subsidiaries. This policy also applies to external service partners and personnel working for the company and any businesses managed by the Group IM of MM.

MMag. Peter Oswald
(CEO)

Mag. Franz Hiesinger
(CFO)

Jacqueline Wild
Head of Group IM