Information Security Policy

Document Title	Information Security Policy
Document ID	MM-ISMS-PL-01
Owner	Nikolaus Brandstetter (CISO)
Approver(s)	Peter Oswald (CEO), Franz Hiesinger (CFO), Roman Billiani (CEO Food & Premium Packaging)
Contact for advice	Information Security security@mm.group
Effective Date	01.02.2018
Last Updated	07.07.2025

Contents

Glossary

Term	Description
Confidentiality	**One of the three core elements of information security, along with integrity and availability. This term refers to ensuring that information is not made available or disclosed to unauthorized individuals, entities, or processes.**
Integrity	**One of the three core elements of information security, along with confidentiality and availability. This term refers to the accuracy and completeness of information and data.**
Availability	**One of the three core elements of information security, along with confidentiality and integrity. Availability concerns the requirement for information, IT systems, people, and processes to be operational and accessible when needed.**
Access control	A generic method of control designed to restrict access to an information asset, permitting authorized access whilst preventing unauthorized access.
Accountable, Accountability	Ultimately answerable for the correct and thorough completion of a task or the protection of information assets. Accountability cannot be delegated, cf. Responsible.
Antivirus	Software designed to minimize the risk of malware by detecting, preventing and/or removing various forms of malware infection such as viruses, worms, trojans, etc. May also control other potentially unwanted software.
Asset	An item that has value to MM, such as money, physical possessions, facilities (machine or computer), people, environment, and intangibles such as reputation.
Audit	Structured process of examination, review, assessment, and reporting by one or more competent people who are independent of the situation, system, process, function, etc. being audited.
Authorize, Authorization	The process of permitting access to a resource, system, or asset.
Awareness	There is no clear definition of awareness in the context of Information Security Awareness. It means to raise awareness of threats to information security and to change the behavior of people.
Breach	Form of information security incident normally occurring because of deliberate action or inaction, as opposed to accidental causes.
Chief Information Security Officer (CISO)	A Chief Information Security Officer (CISO) is an executive responsible for an organization's information security strategy. They oversee the development and implementation of security policies, manage risks, ensure compliance, and protect sensitive data from cyber threats to safeguard organizational assets.
Data Protection	Data protection is the protection of personal data.
Endpoint Detection and Response	Endpoint Detection and Response (EDR) is a cybersecurity technology that focuses on detecting and investigating suspicious activities on endpoints like computers, servers, and mobile devices. EDR solutions help organizations monitor, analyze, and respond to security incidents in real-time to protect against advanced threats and breaches.
Guidelines	Guidelines are explicit recommendations for specific subjects which are not explicitly covered in policies, standards and procedures. These include but are not limited to information security best practices and international standards.
Information	Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected.
Information Assets	An information asset is any data or information that holds value for an organization. This includes databases, documents, software, and intellectual property.

	Proper management and protection of information assets are crucial for ensuring security, compliance, and competitive advantage in the market.
Information Security	Information security refers to the practice of protecting sensitive data from unauthorized access, disclosure, alteration, and destruction. It encompasses processes, technologies, and policies to ensure confidentiality, integrity, and availability of information, safeguarding both personal and organizational assets against cyber threats.
InfoSec	InfoSec, short for Information Security.
Interested Party	Defined as a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Information Security Management System (ISMS)	An Information Security Management System (ISMS) is a systematic approach to managing sensitive company information, ensuring its confidentiality, integrity, and availability. It involves risk assessment, policy development, and continuous improvement to protect data from threats and comply with regulations.
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim.
Multi-factor Authentication	Multi-factor authentication (MFA) is a security process that requires users to provide two or more forms of identification to verify their identity before gaining access to a system or application. This typically involves a combination of something the user knows (like a password), something they have (like a smartphone or security token), or something they are (like a fingerprint or facial recognition). MFA enhances security by adding an extra layer of protection against unauthorized access.
Operational Technology (OT)	Operational Technology (OT) refers to hardware and software which is utilized to control, automate, and monitor systems which are required for the manufacturing of goods.
Password	A password is a secret combination of characters (letters, numbers, symbols) that a user sets up to gain access to a computer, system, application, or account. Passwords are used as a form of authentication to verify the identity of the user and protect sensitive information from unauthorized access.
Plan-Do-Check-Act (PDCA)	PDCA, or Plan-Do-Check-Act, is a continuous improvement cycle used in management. It involves planning a change, implementing it, checking results against expectations, and acting on what was learned to refine processes for better efficiency and effectiveness.
Penetration test	Penetration tests are documented checks and scans on applications, systems, or websites to identify vulnerabilities.
Phishing	Phishing is a social engineering technique. Attackers send forged SMS, e-mails, chat messages, etc. to their victims to get their personal data. After that, attackers can try to impersonate their victims or do something criminal.
Ransomware	Ransomware is a type of malware. The idea is to press victims for money by threatening them with doing something harmful.
Risk	A risk is the measure of the effect of uncertainty on the operations, assets, or individuals. It is based on a measurement of the impact of a threat and the likelihood of the threat occurring.
Risk management	Risk management is the process of the identification, measurement, control, and minimization of risks. It includes assessing risks, taking actions to reduce risks to an acceptable level, and maintaining risks at an acceptable level.
Service Desk	MM's internal service desk support team, reachable via it-service@mm.group or from within servicenow.

Stakeholder	A stakeholder is any individual, group, or organization that has an interest or concern in the security of information within the system. Please see the below table for list of specific types of stakeholders.
Statement of Applicability	The Statement of Applicability or SoA refers to the output from the information risk assessments, and particularly the decisions around treating those risks.
Vulnerability	Vulnerabilities are exploitable security flaws in software or hardware.

Stakeholder Definitions

Term	Description
Authorized Third Party	Authorized third parties are external entities that have been granted permission to access or process the organization's information assets on behalf of the MM group. These could include vendors, service providers, partners, or consultants. An authorized third parties' security practices and controls must align with MM Group's security requirements to mitigate risks associated with third-party access to sensitive data.
Contractors	Contractors are external individuals or organizations hired by MM Group to provide specific services or expertise. Contractors may have access to sensitive information or IT systems, making them important stakeholders whose activities must be managed and monitored to ensure compliance with security requirements and protect the organization's data. All contractors with access to internal resources must abide by the groups policies, procedures and best practices, akin to a standard employee.
Customer	A customer is an external stakeholder who engages with MM Group to purchase products or services. Customers entrust us with their personal or financial information, making them key stakeholders in our ISMS. It is essential to implement security measures to protect customer data, maintain trust, and comply with privacy regulations to ensure the security and privacy of customer information.
Intern	An intern is a temporary employee or trainee who works for the organization for a specific period to gain practical experience. Like a standard employee, an intern is responsible for following security policies, procedures, and best practices to protect sensitive data, report security incidents, and contribute to a culture of security within the organization.
Student Employee	A student is an individual who, alongside their working contract, is enrolled in a program at an educational institution. Like a standard employee, a student is responsible for following security policies, procedures, and best practices to protect sensitive data, report security incidents, and contribute to a culture of security within the organization.
User	A User can be defined as a catch-all stakeholder who interacts with the organization's information systems and data. Users can include employees, contractors, Interns, Student Employees, and any other authorised individuals who access or use the organization's information assets.

1 Purpose

This Information Security Policy lays down the guiding principles for the implementation and operation of the information security management system (ISMS) of Mayr-Melnhof Karton AG (hereinafter MM Group). The purpose of the ISMS is to establish a framework for managing and mitigating risks related to the MM Group information systems and data. The guidelines and procedures the ISMS is built on are there to protect sensitive information and data assets from unauthorized access, use, disclosure, disruption, modification, or destruction. This policy serves as authoritative base for all policies, standards and procedures within MM Group's Information Security Management System (ISMS). As such, abidance to MM Group's Information Security Policy serves as an acceptance to all documents within the ISMS, which are published within the Knowledge Base, available here.

The main goal of an ISMS and this Information Security Policy is to ensure the **confidentiality**, **integrity**, and **availability** of the organization's information assets. It outlines the roles and responsibilities of employees, contractors, and third-party vendors in safeguarding the organization's information assets, across both the IT and OT environments. It also defines the acceptable use of information systems and data, as well as the consequences of violating the policy.

By implementing an Information Security Policy, MM Group can reduce the likelihood of security incidents, such as data breaches, cyber-attacks, and information leaks. It helps to create a culture of security awareness within the MM Group and ensures that employees are aware of their responsibilities in protecting sensitive information.

MM Group offers its employees and clients a safe and secure environment, reduces its environmental impact in general and specifically its impact on climate change while fostering innovation. The climate change related topics are material for the MM Group and assessed regularly by involving internal and external stakeholders.

Overall, an Information Security Policy is essential for establishing a secure and resilient information security program that aligns with the MM Group business objectives and regulatory requirements.

2 Scope

This policy applies to the MM Group including all affiliate companies of MM Group. This document shall apply for an unlimited period from the moment of publication. This policy applies to all employees of MM Group, including full-time, part-time, and temporary employees, contractors, students, interns, and any other authorized third parties who have access to MM Group's data, systems, or processes.

The requirements defined in this policy apply to all data, systems, and services owned and/or managed by MM Group or one of its managed service providers (MSP). The provisions of this document must be implemented across all divisions in the MM Group. The guidelines in this policy also apply to remote work and home offices.

3 Normative basis

Norms, quality standards, regulations and guidelines are binding for the activities of MM Group. The ISMS interacts and overlaps with existing modes of management and thus supports the goal of creating an integrated management system. This applies in particular to the following standards:

- EN ISO 9001:2015
- EN ISO 27001:2022

- EN ISO 27002:2022

4 Information security strategy

MM Group and the management board is aware of the importance of information security, which is why the establishment of our ISMS and the implementation of the associated organizational and technical measures are being promoted. Our information security strategy ensures that legal compliance, business stability and the company's reputation are all upheld to the upmost degree and additionally ensures that the continuous implementation of state-of-the-art security controls and measures is undertaken in an economically responsible manner. A full breakdown of MM Group's information security strategy can be found in here. This document provides a detailed approach to the group's current short-term goals for the group's information security function.

5 Information security objectives

In addition to the defined information security strategy, the group have established a number of objectives which encompass the broader approach to information security which is required across the business. These objectives provide a measurable guidance to the application and understanding of information security controls and provide a suitable baseline for understanding the role of the ISMS within the context of the wider business. As outlined in the Key Performance Indicators and Reporting Procedure document, these objectives allow the Group to track, manage and evaluate the effectiveness of the function of our ISMS.

- Adopt a risk-based approach to ensure that information security risks are treated consistently and effectively.
- Implement full coverage of appropriate security controls and solutions (e.g. Endpoint Detection and Response) across all applicable computational resources within our environments.
- Mitigate information security risk to a manageable level that is accepted by the board.
- Conduct and review the physical security controls and their applicability across sites managed by the group.
- Perform business continuity exercises and documents findings to review MM Group's approach to major incidents
- Track and mitigate vulnerabilities in a manner which is consistent with MM Group's defined vulnerability management procedure, available here.
- Conduct regular penetration tests of MM Group's networks and computational resources, mitigating findings in a timely manner consistent with the vulnerability management procedure.
- Ensure all involved stakeholders are aware of the documented ISMS and track the acceptance of policies in a consistent manner.
- Protect and prevent sensitive information (e.g., customer data) from unauthorized uses or disclosures.
- Conduct risk-based evaluations during the procurement of software and services to ensure the implementation of technology does not undermine the function of information security within the group.
- Conduct application security assessments to identify vulnerabilities and to assess the critically to business operations that specific applications and services hold.
- Foster a security-positive culture in order to continually influence the behavior of all stakeholders to reduce the likelihood and impact of an information security incident.

- Meet legislative/regulatory requirements and audit recommendations in a timely, comprehensive, and fully compliant manner.

5.1 Commitment from management board

The management board of MM Group is aware of the importance of information security and actively supports the company's information security strategy by providing the necessary financial, technical and personnel resources required whilst also monitoring the effectiveness of the implementation of the necessary measures.

The management board of MM Group ensures that information security relevant objectives are identified, adapted to the organizational requirements, and integrated in the relevant processes. Furthermore, the management board of MM Group is responsible that the Group Information Security Policy is drafted, examined, and approved. In addition to the introduction of the Information Security Policy, an important task of the management board of MM Group is also to examine the effectivity of this policy. These duties are periodically performed by conducting management reviews.

The management board of MM Group provides clear instructions regarding security information initiatives and supports the persons responsible in their implementation. Initiating programs and trainings regarding the awareness-raising among employees is an equally important duty of the management board of MM Group as taking responsibility for introducing and monitoring the implemented measures.

5.2 Management review

The management review of the ISMS is an important process that ensures the effectiveness, suitability, and continuous improvement of MM Group's security program. This review takes place at a minimum twice a year. It provides a structured opportunity to assess and enhance the security measures in place, ensuring they continue to meet the evolving needs of the organization. During a management review, key stakeholders, including the management board and the relevant information security roles evaluate the performance of the ISMS and make informed decisions to enhance security measures. In addition to the biannual management review of the ISMS, monthly reports are created by the CISO team and are circulated to the CFO and upon request to any other interested internal party. These monthly reports provide point-in-time tracking of key KPIs and raise awareness to any key updates within the ISMS.

The importance of a management review of the ISMS lies in its ability to:

Assess the ISMS Performance: By reviewing key performance indicators, security incidents, compliance status, and audit findings, the management board as defined in the reporting procedure, available here, can evaluate how well the ISMS is functioning in protecting MM Group information assets.

Identify Improvement Opportunities: Through a thorough analysis of the ISMS processes, controls and outcomes the management review helps identify areas for improvement and corrective actions to address gaps or vulnerabilities in the security program.

Ensure Alignment with Business Objectives: The management review ensures that the ISMS is aligned with MM Group strategic goals, risk tolerance, and regulatory requirements, enabling security efforts to support and enhance overall business objectives.

Promote Accountability and Responsibility: By holding stakeholders accountable for their roles and responsibilities in managing information security, the management review fosters a culture of ownership and commitment to security within the MM Group.

Review and Address Risks: During the management review, identified risks are discussed in detail with management, including the strategies and measures in place to mitigate or treat these risks, ensuring that the organization's risk management approach is robust and effective.

Drive Continuous Improvement: By setting objectives, targets, and strategy based on the findings of the management review, MM Group can drive continuous improvement in its security posture and adapt to evolving threats and challenges.

5.3 MM Information Security Framework

The MM Group information security framework is utilized to implement the relevant controls and processes in order for the group to achieve the objectives outlined in the group's information security strategy. The framework is divided into two main areas, of which tasks are handled by two collaborative teams:

- **Information Security (Governance, Risk, and Compliance):** This area, embedded within the Information Security Team, involves the strategic oversight and management of information security directives. Key components include Context and Leadership, Organizational Culture, Evaluation and Direction, and Compliance and Audit.
- **Security Operations**: The SecOps team works on the practical implementation of security measures. Major aspects include Identity Security, Data Security, Infrastructure Security, OT Security, Change & Support, and Response & Recovery.

Overall, the MM Security Framework represents a holistic approach to information security, integrating both strategic governance aspects and the operational implementation of security measures.

5.3.1 Responsibilities and roles

There are a number of group and individual roles which have direct and indirect responsibilities within the group's ISMS. A full breakdown of each identified role's responsibility can be found within the Roles and Responsibilities Matrix which can be found in this knowledge base document. A brief overview of identified roles is as followed.

- Management board: The management board sets objectives, allocates resources, and monitors the ISMS's performance to ensure alignment with business goals. Individual subsidiaries should also have a management board with similar responsibilities.
- Managing Director of subsidiaries: The Managing Director develops business strategies, oversees financial performance, and drives sustainability initiatives to support company growth.
- Chief Information Security Officer and Information Security Team: The CISO oversees the information security program, while the IS Team provides expertise and operational support to protect MM Group's information assets.
- Information Security Coordinator: The IS Coordinator is a localized role, in which the individuals support the Managing Director/CISO in meeting information security requirements, implementing policies, and identifying vulnerabilities at the site they are response for.
- Chief Information Officer (CIO) and Group Information Management (Group IM) Department: The CIO and Group IM oversee IT strategy and governance, integrating security requirements into various departments to implement and improve the Information Security Policy.

- Security Operations: The Security Operations team ensures security implementation and compliance across various domains within IT Infrastructure to align with industry best practices and regulatory requirements.
- Director Operational Technology (OT): The Director of OT develops and implements OT strategies, collaborates with departments to identify improvement opportunities, and monitors market trends to shape the OT strategy.

5.3.2 Segregation of Duties

Segregation of duties in information security refers to the practice of dividing responsibilities among multiple individuals, ensuring that no single person has control over all aspects of a critical process or transaction, and allocating technical privileges based on the principal of least privilege. By implementing measures that ensure the segregation of duties, the group mitigates the risk of unauthorized activities, intentional misconduct or errors that could compromise the confidentiality, integrity, and availability of information. This practice also helps ensuring accountability, transparency, and compliance with regulatory requirements.

The segregation of duties within the group is implemented by both technical and non-technical measures. A foundational part of the allocation of duties is the principal of least privilege, which defines on an abstract level that level of privilege allocated to a user account should nothing higher that the privilege the user requires to perform their job function. In order to support the proactive application of the principle of least privilege, the group operates role-based access control within Group IM to ensure that access rights to privileged systems are limited to their specific role-based tasks.

5.4 Risk Management

Risks that jeopardize MM Group's ability to uphold its full commitment to information security, therefore threatening the confidentiality, integrity, and availability of MM Group's data and information, must be uncovered and controlled efficiently. All non-financial / operational risks are identified, analyzed, and evaluated through a risk management process. Based on this assessment, decisions are made on how to manage each risk. It is important to note that not all identified risks need to be prevented; some risks could be accepted based on operational considerations, cost-effectiveness, or the impact of risk mitigation measures on production processes.

By identifying risks and opportunities at MM Group, the goal is to proactively identify potential threats to the company's sustainability and implement timely risk reduction measures. Simultaneously, the aim is to leverage opportunities to enhance processes and products.

More information can be found in the Risk Management Standard, which is published in ServiceNow within the Governance, Risk, and Compliance Knowledge Base here.

5.5 Exception to the policy

Exceptions to the policy and controls must be discussed with and approved by the CISO and are evaluated case by case.

Regarding the operational environments within the group, it is vital to note that the physical safety of our employees is paramount above the regulations and controls defined within the group's information security management system. As such, should there be a serious threat to the safety of individuals present at a MM Group site

and non-compliance to any control within our ISMS is deemed necessary to ensure their safety and avoid bodily harm, there will be no sanctions imposed on the individual(s).

5.6 Plan Do Check Act-Process

The established ISMS is examined using recognized methods and indicators regarding effectiveness and efficiency. The fulfillment of defined objectives is ensured by the Plan-Do-Check-Act (PDCA) process of the ISMS.

The PDCA cycle is a four-step management method used for continuous improvement in various processes, including ISMS.

Plan: In this phase, objectives and processes necessary to deliver results are established. This involves identifying risks, defining controls, setting policies, and planning improvements.

Do: The implementation of the plan is carried out in this phase. This involves executing processes, implementing controls, and training employees on security protocols.

Check: In this phase, the performance of the implemented processes and controls is monitored and evaluated. This includes conducting audits, assessments, and reviews to ensure compliance with policies and standards.

Act: Based on the results of the checks, actions are taken to improve processes and controls further. This could involve updating policies, refining procedures, or implementing additional security measures.

It is essential to incorporate the PDCA cycle into an ISMS because information security is a dynamic and evolving field. Threats, vulnerabilities, and technologies change rapidly, requiring organizations to continuously assess and improve their security measures. By following the PDCA cycle, organizations can adapt to new challenges, enhance their security posture and ensure that their ISMS remains effective and efficient over time.

The PDCA cycle is not a one-time activity but a continuous process that organizations should regularly revisit to stay ahead of emerging threats and maintain a robust information security posture. By cyclically planning, implementing, checking, and acting on improvements, organizations can achieve ongoing security resilience and adaptability in the face of evolving risks.

5.7 Dealing with vulnerabilities

Managing vulnerabilities within an ISMS is essential for maintaining the confidentiality, integrity, and availability of sensitive information. Identifying and addressing vulnerabilities proactively helps prevent potential security breaches and data leaks that can have severe consequences for the MM Group. Vulnerabilities in the system can be exploited by malicious actors to gain unauthorized access to critical data and compromise the organization's security posture. Regular vulnerability assessments and scans are necessary to identify weaknesses in infrastructure or applications and prioritize remediation efforts based on the level of risk they pose. By managing vulnerabilities effectively, MM Group can reduce the likelihood of cyber-attacks, data breaches, and financial losses. Patch management and updates are crucial for addressing known vulnerabilities in software, applications, and systems to keep them secure and up to date. Failure to manage vulnerabilities can result in compliance violations, reputational damage, and legal consequences for the organization. Implementing a robust vulnerability management program within the ISMS helps strengthen the MM Group overall security posture and resilience against emerging threats. Continuous monitoring and mitigation of vulnerabilities are key components of a proactive and effective information security strategy.

More information can be found in the Vulnerability Mitigation Procedure, which is available here.

5.8 Regulations, laws and treaties

Regulations, laws and contracts are systematically taken into account in the ISMS in order to fulfill legal and regulatory requirements. This is done by identifying relevant regulations, integrating them into security guidelines and training employees. Regular audits and adjustments ensure continuous compliance, minimize legal risks, and protect the integrity of information and the confidentiality of sensitive data. These are regularly maintained by Group Legal.

5.9 Contact with authorities

Contact with authorities within an ISMS involves establishing clear protocols for communication with relevant regulatory bodies, law enforcement, and industry organizations. This process ensures compliance with legal requirements and promotes swift reporting of security incidents. Establishing a designated point of contact helps facilitate effective collaboration during investigations or audits, while maintaining transparency and accountability.

5.10 Contact with special interest groups

Contact with special interest groups in the context of an ISMS involves engaging stakeholders who influence or are affected by the organization's information security policies. These groups can include regulatory bodies, industry associations, and community organizations. Effective communication fosters collaboration enhances awareness of security challenges and aligns security strategies with broader social and legal expectations, ultimately strengthening the organization's commitment to protecting sensitive information and ensuring compliance. Relevant interested parties can have requirements related to climate change, given the impact that the usage of technology has on the environment. For further information on the identification of special interest groups at MM Group, please refer to the ISMS Scoping document.

For further information on the data privacy coordinators within the business, please refer to the site maintained by Group legal, available here. To view the responsible Information Security stakeholders for a specific site, please refer to this page.

5.11 Security training and awareness-raising measures

Awareness training in information security is crucial for both new and existing employees to ensure they are well-informed about security policies, best practices, and potential threats. For new employees, this training educates them about the security protocols, while for existing staff, it keeps them updated on evolving security risks and reinforces good security habits.

For further information on the Group's security training and awareness procedures, refer to the Security Awareness and Training Standard.

6 Non-compliance

The management bodies bear responsibility for ensuring that the ISMS regulations are implemented. Compliance with ISMS regulations will be actively monitored and will be subject to inspection. Violations of this policy will be

treated like other allegations of wrongdoing at MM Group and will be investigated per established procedures. If it is determined that employees are not observing the ISMS regulations, the relevant management bodies shall instruct these employees regarding their obligations. Where appropriate, sanctions will be imposed in case of non-compliance. Sanctions may include, but are not limited to, one or more of the following:

- Oral and/or written warning
- Probation, suspension, or termination of employment
- Legal action per applicable laws and contractual agreements

7 Reporting Violations

If a user becomes aware of a possible violation of this standard, he or she must report it to one of the communication lines below. It is essential and mandatory that in the event of a suspected breach of a policy or a standard, or of a breach of any of the Group's regulatory requirements, the CISO Team must be informed as soon as possible. It is therefore recommended to contact the CISO team at the earliest opportunity. If the CISO team is not initially informed, it is the responsibility of the informed individual's supervisor or the IT representative to ensure the information is cascaded to the CISO team.

- **Recommended First Port of Call**: ServiceNow incident reporting tool
    - MM Group CISO and Security Operations teams can alternatively be reached at security@mm.group
- Immediate supervisor
- Local IT department, local Internal Security Coordinator, or the service desk

8 Statement of liability

The management board of the MM Group and the Head of Group IM define principles on which all decisions and measures regarding IT and OT issues within the company must be based. This policy is derived from the overall group strategies and harmonized with these strategies. It is an essential component in achieving corporate objectives and implementing the defined Governance, Risk & Compliance (GRC) strategy. The MM Group is committed to realize and maintain this information security policy and improve its effectiveness continuously.

This information security policy, as well as the associated standards and procedures, are approved with effect from September 1st 2025, enter into force, and are declared binding upon all employees of MM Group including all affiliate companies of Mayr-Melnhof Karton AG.

MMag. Peter Oswald (CEO)	Mag. Franz Hiesinger (CFO)	Roman Billiani (CEO Food & Premium Packaging)	Nikolaus Brandstetter (CISO, ISMS Owner)

9 Related Documents

All current ISMS documents are available here.

10 Revision History

Version	Change	Author	Date of Change
1.0.	First Version	Marcel Lehner	01.02.2018
2.0	Strategic alignment	Marcel Lehner	01.07.2021
3.0	New creation, revision of the entire Policy	Jennifer Nussbaumer	27.08.2024
4.0	Revision of Policy in line with ISO 27001:2022	Nikolaus Brandstetter, Ben Skelding, Jennifer Nussbaumer, Martin Fridl (external)	12.03.2025
4.1	Revision of Policy in line with feedback from internal parties	Nikolaus Brandstetter, Ben Skelding, Andrijana Grabovica	07.07.2025