Information security policy

Contents

Contents **2**

1. Mission statement **3**

1.1. Information security culture *3*

1.2. Objectives of information security *3*

1.3. Information security strategy *4*

2. Scope, integration in the company **4**

3. Principles **4**

4. Enforcement and sanctions **5**

5. Statement of liability **5**

1. Mission statement

Mayr-Melnhof Karton AG (subsequently also “MM Group” or “MM”) is the world’s largest producer of coated recycled cardboard, as well as Europe’s leading manufacturer of folding cartons. The strategic orientation of the MM Group is based on four pillars: concentration on core competencies, market and cost leadership, long-term profit orientation and expansion.

Information and communication technology equipment and practices are a significant factor in implementing these strategic objectives. These technologies are necessary to carry out internal procedures as well as procurement activities and the deliveries and services for our customers in a timely and cost-efficient manner, ensuring the necessary quality. There is also a high dependency on secure information processing, available at all times. The functionality and availability of the information technology systems and networks, as well as the confidentiality and integrity of business processes and data, are exposed to the constant risk of technical faults, misconduct, sabotage and espionage. This may lead to a loss of image, commercial damage and, in extreme cases, endangerment of the environment and human health.

In view of this, information security is a high priority at MM Group. The company therefore operates an integrated information security management system (ISMS), which safeguards confidentiality, availability, integrity and authenticity in an effective, sustainable and cost-effective manner.

1.1. Information security culture

Our customers’ confidence in the quality and security of our services is of great importance to MM Group. This includes the data and information that is needed for the safe operation of the office environment and technical equipment, as well as the data and information generated by customers and processed as personal data. MM Group takes all necessary and commercially viable measures to protect its services, systems, data and information in accordance with the state of the art[1].

This information security culture forms part of the corporate culture at MM and defines awareness, thinking and action in relation to information security. It is therefore one of the informal structures and is consistently applied, further developed and communicated to employees by the management bodies.

1.2. Objectives of information security

In order to meet the requirements of the framework conditions and security culture, MM Group has defined following objectives for information security:

- Framework conditions should be created to protect services, systems, data and information against manipulation or theft in accordance with the state of the art.
- Framework conditions should be created to ensure that, when new technologies are used, information security is included in a risk-based evaluation for procurement and operations with the same importance as cost-effectiveness and usability.
- Framework conditions should be created to enable MM Group to meet statutory information security and data protection requirements in a timely, comprehensive and fully compliant manner.

[1] For a definition of *state of the art*, see “Abbreviations and definitions”

1.3. Information security strategy

The strategy for implementing these objectives includes the following aspects:

- Expanding the internal control system for information security aspects.
- Developing an information security management system (ISMS) in accordance with internationally recognised standards.
- Developing an information security risk management system (IS-RM) that provides the company management with information to enable risk-appropriate decisions to be made in matters relating to information security.
- Establishing a training and awareness programme to align technical IS knowledge and IS awareness with current requirements.
- Establishing appropriate key performance indicators (KPIs) and auditing measures to enable the continuous measurement and improvement of operational effectiveness and the quality of the ISMS, as well as the operational and technical measures put in place.
- Establishing processes for the communication required by law with authorities and customers regarding any security incidents or to request personal data and information.

2. Scope, integration in the company

This policy applies within Mayr-Melnhof Karton AG and all of its subsidiaries, regardless of location, and relates to all activities, functions, processes, assets and information assets that are necessary to achieving the corporate objectives. This policy must be brought to the attention of all contractors and applies to the procurement of new IT systems. For example, this is achieved by applying the corresponding provision in the purchase conditions or planning documents. In addition, the regulatory content of this policy may be taken into account in the individual contract. All employees are obliged to observe and apply the principles set out below and the related standards in the planning, development, procurement, creation, operation and disposal of information assets.

3. Principles

The information security management system is based on standard ISO/IEC 27001:2013 and BSI standards and continuously developed, whereby the following principles must be taken into account:

- The information security measures and information security risk management process can be clearly and unambiguously derived from the information security policy.
- Every employee should receive the information needed to fulfil his/her duties. Technical or organisational measures must be used to prevent an excess of information from being provided. To ensure an approach that prevents errors and manipulation by individuals, incompatible functions, roles and responsibilities must be separated. This functional separation should separate implementation activities from the monitoring of the operational effectiveness of these activities. If functional separation is not possible, measures must be taken to compensate for this. These measures must be approved by the management bodies.
- Access to information is logged. Access to information is explicitly regulated during the distribution of tasks.
- Compliance with the principles, as well as the operational effectiveness of the information security management system, is checked as part of internal and external audits and during regular risk analyses. The results are documented. Concrete measures are derived based on the documentation.
- The specific information security measures to be implemented are chosen in proportion to the risks. The state of the art is taken into account for the implementation of the measures. A continuously evolving

innovation process is used to regularly review and adapt the state of the art.

- An approach combining basic protective measures and detailed risk analysis is used to establish a risk-appropriate security level.
- Data and information is classified in relation to confidentiality, integrity, availability and data protection relevance.
- Employees receive regular information regarding the necessary knowledge for consciously handling information, via training and awareness-raising measures.
- The relevant principles are set out in company guidelines and organisational instructions.
- ISMS requirements are immediately applicable to newly implemented IT systems. A separate transition will be agreed for existing systems.
- An appropriate system of indicators must be maintained for the continuous development of the information security management system.

4. Enforcement and sanctions

The management bodies bear responsibility for ensuring that the information security measures are implemented. Compliance with the information security measures will be actively monitored. If, based on these checks, it is determined that employees are not observing the information security measures, the relevant management bodies shall instruct these employees regarding their obligations. Where appropriate, sanctions will be imposed in case of non-compliance.

5. Statement of liability

In version 1.10 of this information security policy of 1 February 2018, the management board and IT management of MM Group define principles on which all decisions and measures regarding IT issues within the company must be based. This policy is derived from the overall group strategies and harmonised with these strategies. It is an essential component in achieving corporate objectives and implementing the defined IT strategy. The MM Group undertakes to realise and maintain this information security policy, and to continuously improve its effectiveness.

This information security policy, as well as the associated guidelines and work instructions, are approved with effect from 1 March 2018, enter into force and are declared binding upon all employees of Mayr-Melnhof Karton AG and all subsidiaries majority-owned by Mayr-Melnhof Karton AG (including external employees working for the company and all companies serviced by corporate IT of MM Group).

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