Information Security Policy MB 13-0-02

ROLE	NAME	POSITION	DATE
Creation	Marcus Korte	Corporate Information Security Officer	13.04.2018
Approval	Lorenz Zwingmann	Chief Financial Officer	04.07.2018

CONTENTS

1.1 Ownership & Management

Owner	*Lorenz Zwingmann*	*Member of the Executive Board of M&B AG*
Approval by	*Lorenz Zwingmann*	*Member of the Executive Board of M&B AG*

REVISION	
Next review	by 01 January 2020
Last changed	Klicken Sie hier, um Text einzugeben.

REFERENCE	
Document type	Policy
Document no.	*MB 13-0-0-02*

Code of Conduct
Data Protection Policy (under development)

2 Information Security at the Marquard & Bahls Group

The ongoing evolution of information and communication technology (ICT) opens up new advantages and opportunities in our business activities. These include, for example, global networking in all our processes, for an efficient exchange of information with our business partners. The resulting increasing digitization of processes and the constantly growing demands on ICT are accompanied by many dangers and risks. Effective information security processes are essential prerequisites for countering today's dangers and protecting our information assets. For this reason, Marquard & Bahls has set up an Information Security Management System (ISMS). This Information Security Policy describes business requirements, legal, contractual and other regulatory requirements, basic principles and objectives, as well as the obligation to comply with these needs and requirements. It is supplemented by the applicable guidelines and standards that explain our information security measures in detail.

Beside this Information Security Policy a dedicated Data Protection Policy will be released and outline the organization of data protection.

3 Scope

This Information Security Policy applies to Marquard & Bahls AG and the companies directly or indirectly controlled by it ("M&B Group" or "the Company"), as well as all respective M&B Group Employees and third parties.
Binding regulations and organizational measures to ensure the required information security are also a compliance requirement. This includes, for example, data protection regulations, information security regulations, and industry-specific regulations. All our business partners are required to protect information as part of their responsibilities and processes.

4 Importance of Information Processing

Information processing has come to play a key role in our various business activities.
All key strategic and operational processes are significantly supported by ICT.
Any failure of ICT infrastructures must be able to be compensated for at short notice. Even in the event of partial failures of the ICT infrastructure, our critical services must be available and our business activities must be able to continue.
The protection of our information against unauthorized access or unauthorized modification is of vital importance.

5 Information Security Objectives

As a responsible company, Marquard & Bahls undertakes to conduct all business activities securely and efficiently. The Information Security Objectives (confidentiality, integrity, authenticity and availability) form the basis for protecting information and fulfilling this obligation.

5.1 Confidentiality

The trust of our business partners and our business success are based on our ensuring a conscientious handling of confidential information and the protection of trade and business secrets. Data protection laws and the interests of our employees, too, require protective measures to ensure the confidentiality of our data. The same goes for our customers and business partners' data.

5.2 Integrity and Authenticity

The integrity and authenticity of our business processes, information assets, and actions ensure the reliability of our global business transactions. Our business partners depend on the completeness and accuracy of our information assets, including the supporting ICT, in our processes.

5.3 Availability

Timely action, e.g. as stipulated by contractual obligations, requires the availability of information assets.

Security measures must be handled in a risk-driven manner. Damage claims with heavy financial consequences must be prevented.

The importance of these values is highlighted in our Code of Conduct as well.

6 Basic Principles of Information Security

To achieve the Information Security Objectives, an ISMS was set up and principles were agreed to maintain a defined level of protection. This includes:

6.1 Information Security as a Performance Feature

Information security is a controlling performance feature at the Marquard & Bahls Group. Any identified risks are to be addressed in the implementation of projects. Matters of information security concerns must be considered e.g. in:

- compliance with laws and regulations
- the establishment of services
- the procurement, commissioning and disposal of information assets
- the use of third-party services
- implementing state-of-the-art technology: As the operator of a critical infrastructure we are obliged to use state-of-the-art technology to ensure that we fulfil our service mission.

6.2 Information Security as a Performance Feature of the Organization

Technical and organizational security measures shall be designed in such a way that they are always an integral part of all business processes.

Matters of information security concerns must be considered e.g. in:

- the details of the organization
- creating and filling functions and roles
- managing employees
- training and continuing education
- workflow design
- cooperation with other [public] authorities and third parties
- selecting and using tools

All this is based on the principle of the informed and responsible employee. To this end, employees shall be trained, sensitized and qualified to the necessary extent with regard to information security. Responsible conduct by employees is to be encouraged.

6.3 Risk Management Processes

Information security aspects are to be considered in risk management processes at the Marquard & Bahls Group.
Aspects to be evaluated include the effects of hazards on

- People's physical and mental intactness
- the right to informational self-determination,
- financial damages
- reputational impact
- consequences of violations of the law

The necessary resources (personnel, equipment and investment funds) shall be made available to implement the necessary and appropriate security measures.

The "all-hazards approach" applies. A risk management and action plan is decided and implemented as a result of the latest risk analysis.

7 Responsibilities

7.1 Management Responsibilities

Information security is a management task that affects the entire company.
It is therefore in the interest of management to

- take responsibility for the objectives and principles formulated in the Information Security Policy and to anchor them throughout the organization
- approve and provide sufficient resources for establishing a sustainable ISMS
- take responsibility for the risk management, operational information security measures and business continuity strategy.

One key factor for successful information security is the visible and full support and commitment of all levels of management. Management should therefore actively support the implementation of this Information Security Policy within the organization by issuing clear guidelines and instructions and recognizing responsible behavior.

7.2 Line Managers' Functions

For business processes or specialized procedures, line managers shall be appointed who are responsible, in the area of responsibility assigned to them, for

- determining the business relevance and security needs of the information processed
- ensuring that responsibilities are explicitly defined, and that security and control measures to manage and protect the information within their area of responsibility are implemented

The line manager must define the access to information as well as the scope and type of authorization required for a given procedure. In making these decisions, the following shall be considered:

- the need to protect the information, according to its business relevance
- the storage regulations and legal requirements associated with the information
- the necessary accessibility of the information required for the respective business requirements

In addition, he is responsible for the implementation and compliance with the policies (policies, guidelines, procedures) and locally derived policies in his area of responsibility.

7.3 Employee Responsibilities

All employees shall safeguard information security by acting responsibly, and shall comply with the laws, regulations, guidelines, instructions and contractual obligations relevant to information security. They shall deal correctly and responsibly with the information assets they use. Among other things, this means

- the obligation to maintain confidentiality in compliance with data protection laws and other regulations

- Using information and information systems only for the purpose of the assigned tasks
- Exercising due care in handling this information
- Only using information systems, components and applications (software) that are provided or accredited by the employer
- Compliance with applicable information security regulations
- If necessary, jointly defining the information security requirements for important and sensitive information with the supervisor, in compliance with the associated guidelines and laws
- Reporting vulnerabilities or incidents affecting the information security using the established communication channels to a supervisor, the Corporate Information Security Officer (CISO) or, in regards to personal data, the Data Protection Officer

7.4 Responsibilities of Third-Party (External) Service Providers

Business partners and third parties who are not part of the Marquard & Bahls Group, but who provide services for them, must comply with the client's requirements for compliance with the Information Security Objectives in accordance with this and other specific policies. The client shall inform the contractor of these rules and oblige the contractor to comply with them in an appropriate manner. This includes the contractor’s duty to inform the client in the event of discernible deficiencies and risks of the security measures used.

8 Information Security Organization

8.1 Corporate Information Security Officer (CISO)

The senior management shall appoint a Corporate Information Security Officer (CISO) to serve as the central security authority for the Marquard & Bahls Group. The CISO is responsible for maintaining the ISMS. A direct reporting channel to the company management shall be ensured for the CISO.

The responsibility of the individual company divisions for information security within the scope of their tasks remains unaffected by this.

The CISO performs the following tasks:

- Manage the ISMS
- Review the information security requirements
- Prepare , update and implement further regulations derived from this policy
- Propose new security measures and strategies
- Represent Marquard & Bahls in information security-related matters
- Serve as a contact person for employees in matters of information security
- Coordinate awareness-building and training measures
- Promote cooperation on information security across the Marquard & Bahls Group
- Report of particularly security-relevant incidents via their reporting channels.

8.2 Group Information Security Board

To support the ISMS in achieving its information security objectives and as Information Security Steering Committee / Information Security Governance Body the Group Information Security Board is established.
It gives the strategic direction for the Group Information Security approach as well.

Beside the functional representatives like

- Human Resources
- IT
- Internal Audit
- HSSE
- Legal and Data Protection
- Compliance

the CFO as board representative and business representatives will be participants.

8.3 Information Security Management Teams (Committees)

To support the ISMS in achieving its information security goals, ISMS teams shall be established with the aim of safeguarding matters of information security in strategic decisions or more extensive projects.

In addition to the CISO, these include

- the company management
- the project manager and their deputy
- Representatives of the group companies as specialists from the respective divisions (e.g. Oiltanking, Mabanaft, Skytanking and also specialist departments such as HSSE)
- Internal Audit and Compliance
- the Data Protection Officer
- Continuity management officers

The tasks result from the ISMS management processes. The Information Security Management Team regularly reports to the company management on the status of information security.

8.4 Policies

The CISO defines in negotiation with the Group Information Security Board policies and guidelines for information security and monitors the implementation.

9 Safeguarding and Improving Information Security

The information security process shall be regularly reviewed for its up-to-dateness and effectiveness. In particular, the measures shall be regularly examined to determine whether the affected employees are aware of them, whether they are feasible, and whether they can be integrated into the business processes. The company management shall support the continuous improvement of the security level. Senior management is committed to communicating changes in corporate strategy that will have an impact on the interests and objectives of information security. A regular monitoring of the ISMS and review of the Information Security Objectives shall ensure the desired level of information security.

10 Deviations

Deviations from this security policy require prior approval by the owner.

Local guidelines or procedures may be published without prior approval if their aim is compliance with these guidelines and the identical standards.

11 Non-Compliance

11.1 Consequences of Non-Compliance

Intentional or grossly negligent actions that endanger information security shall be treated as information security incidents.

These include:

- Falsification of information
- Unauthorized access to information, as well as unauthorized transmission
- Illegal use of company data
- Compromising of information assets

Intentional violations of this security policy and other guidelines officially adopted by management may have disciplinary, labor, civil or criminal law consequences, which may include assertion of liability and recourse claims.

11.2 Reporting Suspected Violations (Whistleblowing)

Any employee who has reason to believe that a violation of this policy has occurred or may occur must report this information to their supervisor, the CISO, the next supervisory level, or the Group Compliance Team.

Alternatively, information can be reported via the Marquard & Bahls CARE platform as described on the Marquard & Bahls website and intranet. Retaliatory measures in any form against an employee who has reported in good faith a violation or possible violation of this or other policy / guidelines are strictly prohibited.

12 Definitions

TERM	DEFINITION / EXPLANATORY REMARKS
CISO	Corporate Information Security Officer
ICT	Information and Communications Technology