
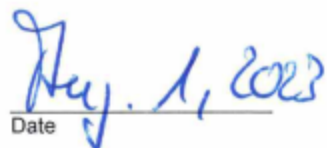

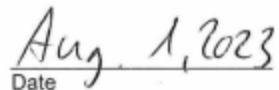




Information Security Policy

Applicable to: Dürr Group

Functional approval:	 _____ Dirk Fleischer, Corporate Security, Dürr AG	 _____ Date
Quality approval:	 _____ Fabian Mock, Corporate Internal Audit, Dürr AG	 _____ Date
Overall approval:	 _____ Dr. Jochen Weyrauch, CEO, Dürr AG	 _____ Date

Distribution and/or duplication of this document, modifications to it and informing others of its content are prohibited unless expressly permitted. Any violations will entail liability for damages. All rights reserved in the event of application for a patent, utility model patent or design registration.

Modification status

Update service

This document is currently not subject to an update service.

Corporate Internal Audit (CIA) - maintains an update service for this document.

The latest version of this document is available on the DÜRRnet.

Update status

Document Version: 2.0 dated 01. Aug. 2023.
The history of previous versions is listed below:

Version	Date	Change/reason
1.0	8/24/2020	First Version
2.0	4/19/2023	Document review (Adaptation of Responsibilities, Format)
2.0	01. Aug. 2023	Update Functional Approval

Content

1	Guiding Principle and Importance of Information Security	4
2	Implementing an Appropriate Level of Information Security	6
3	Responsibility of the Management	7
4	Final Provisions and Scope	8

1 Guiding Principle and Importance of Information Security

As one of the world's leading firms for innovative technology, specific know-how is extremely important in the Dürr Group and therefore subject to a special need for protection. Only by effectively protecting this information can economic success be sustainably secured.

Beyond that, our company also has responsibility towards its customers. Confidential information supplied by business partners is handled confidentially and used only for the agreed purpose. Obligations and agreements made in respect of special confidentiality are complied with at all times.

Effective and comprehensive protection of this information is based on a comprehensive risk assessment and an equally comprehensive security concept which not only includes IT measures but also involves all relevant areas of the company.

The goal of an integrated Information Security Management System is to ensure the effective protection of information requiring protection across all areas of the business.

The ISMS is established on the basis of the following guiding principles:

- Business-based approach
 - The information protection arrangements of the Dürr Group are based on the business obligations and requirements of the company. They ensure economic success and reduce risks for the corporate group.
- Risk-based approach
 - Main areas of focus are defined so that risks are identified and reduced according to their potential to cause damage and the probability of them occurring.
- Uniform approach
 - All employees in the Dürr Group are jointly responsible for information security. The consistency of effective information protection arrangements is guaranteed by uniform standards and processes.
- Process-based approach
 - The ISMS follows the continuous improvement process recommended in ISO/IEC 27001 on the basis of the Deming cycle model (Plan, Do, Check, Act). The goal is to regularly ensure on the basis of evidence the appropriateness, completeness, sustainability, effectiveness, and efficiency of the implemented information security processes and protective measures within the Dürr Group.

In order to fulfill this goal and the guiding principles, the ISMS defines a necessary, suitable, and appropriate level of security with regard to the

- Confidentiality – Protection of valuable or sensitive information against unauthorized access/disclosure;
- Integrity (correctness) – Protection of valuable or sensitive information against intentional or unintentional falsification in order to ensure correctness and completeness;
- Availability – Ensuring that the processing procedures of information are made available in accordance with the time requirements of staff and business partners;

of business processes, data, information, and IT systems.

In order to guarantee confidentiality:

- Information in need of protection is identified and classified
- Access to the information is restricted (need-to-know principle)
- Sufficient protective measures are taken (the more critical the information, the more intensive the protection)

In order to guarantee integrity:

- Data are protected against unauthorized/unwanted modification by means of technical and organizational security measures
- Access rights and roles are defined and complied with
- The correctness of information is regularly checked

In order to guarantee availability:

- Redundancies are created where necessary
- IT systems are secured according to the state of the technology
- Weak areas are identified and eliminated

2 Implementing an Appropriate Level of Information Security

All considerations in respect of the ISMS are based on the principle of the integrated management systems used in the group under the responsibility of the respective management staff.

The Dürr Group uses a globally implemented Information Security Management System (ISMS) based on the international standard ISO/IEC 27001 to guarantee the implementation of information security requirements.

Company-specific information security requirements are handled and implemented in consideration of globally defined stipulations and standards on information security in the locally established organizations and processes of the companies.

The process-based approach is implemented on the basis of the Deming cycle, which is defined as follows:

PLAN - Define the ISMS: The strategies, objectives, processes, regulations, procedures, methods, tools, and responsibilities of the ISMS are defined.

DO - Implement and execute the ISMS: The defined processes, regulations, and procedures are implemented in accordance with the objectives of the ISMS. Selected measures are implemented.

CHECK - Monitor and check the ISMS: The processes, effectiveness, and efficiency of the selected approaches and measures are gaged and checked on the basis of practical experience, the results of audits, and management evaluations. It is identified whether there is a need for action and where room for improvement is present.

ACT - Maintain and improve the ISMS: Based on the results of the Check phase and other feedback (e.g. current risk situation / threat situation / further developments / requirements), corrective and preventive measures are taken that result in the continuous improvement of the ISMS and the security level.

3 Responsibility of the Management

The board of management of Dürr AG, the boards of management of the subgroups, and all managing directors of the group companies are responsible for information security within their respective remit and obligated to provide the required staffing, organizational, and financial resources to establish, maintain, and further develop an appropriate level of information security.

Within the scope of their management tasks and function as role models, all management staff are to a particular degree responsible raising for promoting and maintaining the awareness and discipline of their staff with regard to information security.

4 Final Provisions and Scope

This policy is supplemented with other management processes and guidelines. These include detailed organizational and security rules for areas with different requirements for information security as well as country or location-specific statutory and organizational regulations.

Further information on this can be found in the document “Scope of the Information Security Management System (ISMS)”.