Global Information Security and Data Protection Policy

24.07.2026

In an increasingly digitalised world, the protection of information, data, personal data, and IT systems is becoming increasingly important. The security of these assets is essential to maintaining the trust of our customers, partners, and employees and to complying with legal and regulatory requirements. This Information Security and Data Protection Policy expresses the positive attitude, interest, and sense of responsibility of the Scheidt & Bachmann companies with regard to information security and data protection.

The Information Security and Data Protection Policy applies to the entire Scheidt & Bachmann group, in particular to those Scheidt & Bachmann companies that have established an information security and data protection management system. The management systems are each operated as a central multi-site management system and cover all Scheidt & Bachmann companies and sites that are, or will be, included within the defined scope of the respective management system.

Scheidt & Bachmann's business activities essentially depend on information technology and the associated data and systems. As a globally active group of companies, we are responsible for ensuring the confidentiality, integrity, and availability of the data processed within the Scheidt & Bachmann group and the systems operated, and for eliminating the risks to the rights and freedoms of natural persons arising from the processing of personal data. Compliance with these protection objectives is of great importance to Scheidt & Bachmann.

For Scheidt & Bachmann, a high level of information security and data protection is essential to ensure the functionality and performance of our business processes. It is therefore of utmost importance to ensure information and data security at an appropriate level.

The information processing systems and the information respectively data processed must be protected in such a way that

- they and the business processes that depend on them are available in accordance with requirements,
- their integrity is ensured, and
- the confidentiality is maintained in an appropriate manner.

We consider it an important task to identify information security risks and control them through appropriate action, i.e. to reduce them to an acceptable level or avoid them altogether. The legal and regulatory framework provides the minimum criteria for this.

Our goal is not only to ensure information and data security at a risk-oriented level, but also to continuously improve it. To achieve this goal, we operate an information security management system (ISMS) in accordance with DIN EN ISO/IEC 27001:2024 and a data protection management system (PIMS) in accordance with DIN EN ISO/IEC 27701:2026, in their currently valid versions. The

ISMS and PIMS are organised as certified multi-site management systems. Under both management systems, central guidelines are implemented, monitored and continuously improved by the organisational units and sites responsible at local level. In doing so, we ensure that all requirements of the standards are correctly implemented, that the information security and data protection objectives are aligned with the company's objectives and that the processes and protective measures within the management systems are continuously improved.

Scheidt & Bachmann undertakes to provide all information and resources necessary to achieve the strategic and operational objectives of information security and data protection management. To this end, we undertake in particular

- to continuously review, evaluate, and improve the performance of Scheidt & Bachmann, of the ISMS and of the PIMS related to information security and data protection;
- to provide the necessary resources to achieve the strategic and operational objectives;
- to promote information security and data protection awareness among our employees through training, information and by setting an example in our own actions;
- to comply with applicable legal, contractual, and other requirements regarding information security and data protection and, in particular, to fulfil the role of the controller or processor.

The above commitments form the foundation for establishing and maintaining a high level of information security and data protection at Scheidt & Bachmann. To ensure the effectiveness of these principles, we also strive for measurable progress and verifiable processes in relevant areas.

The following points list areas in which we set quantitative targets or collect quantitative indicators to promote and monitor compliance with our principles:

- Expansion of the scope of DIN EN ISO/IEC 27001:2024: By 31.12.2030, 100 % of the Scheidt & Bachmann companies defined in the certification programme are to be certified to DIN EN ISO/IEC 27001:2024. Progress towards this target is measured annually on the basis of the proportion of certified companies and assessed during the ISMS Management Review. The scope of certification is reviewed and updated annually.
- Training on internal ISMS and PIMS guidelines: By 31.12.2027, at least 90 % of staff shall have attended the compulsory training courses on relevant ISMS and PIMS topics. Progress towards this target will be measured annually on the basis of the training participation rate and assessed during the management review. The participation rate achieved will then be maintained on an ongoing basis and reviewed annually.

The Scheidt & Bachmann ISMS resp. PIMS manual and other documents and processes specify information security and data protection management and are binding for all Scheidt & Bachmann employees.

In order to maintain and restore business processes in the event of security incidents, disasters, or other disruptions, the establishment of a business continuity management based on international standards (e. g. ISO 22301, BSI 200-4) is an important part of the security strategy.

Top management (Group CEO) bears overall responsibility for the group-wide ISMS and PIMS, and for compliance with information security requirements.

A Chief Information Security Officer has been appointed to oversee the strategic and operational implementation of the ISMS and bears overall responsibility for information security within the Scheidt & Bachmann Group.

The appointed Data Protection Officer of Scheidt & Bachmann GmbH is responsible for the strategic and operational implementation of the PIMS and for data protection within the Scheidt & Bachmann Group.

The managing directors and managers of the individual Group companies and sites are responsible for site-specific implementation of this policy and for derived guidelines, processes, procedures, standards, concepts and measures, and they provide the necessary resources. All employees, including executive management and managers with their role model function, are responsible for complying with this policy.

All departments of the Scheidt & Bachmann group whose actions have a significant influence on the achievement of our goals are responsible for achieving them. For the quantitative targets mentioned, these are the employees of the IT Infrastructure & Client IT Services department, the Information Security Officers, the Data Protection Coordinators, the designated employees and the management at the national/ international sites who are involved in the implementation and maintenance of the ISMS resp. PIMS, as well as the Data Protection Officer and the Chief Information Security Officer.

The appointed Information Security Officers of the individual business divisions and companies assume the role of local representatives within the multi-site ISMS. They ensure that the centrally defined requirements of the ISMS are implemented fully, effectively and in an auditable manner at their respective sites. The Information Security Officers are supported in their respective business divisions and companies by the Chief Information Security Officer and by the ISMS teams established for each division.

The appointed Data Protection Coordinators for the individual business divisions and companies assume the role of local representatives within the multi-site PIMS. They ensure that the centrally defined requirements of the PIMS are implemented fully, effectively and in an auditable manner at their respective sites. The data protection coordinators are supported within the respective business divisions and companies by the Data Protection Officer and by the respective PIMS teams.

In accordance with our company values – in particular the value of "trust & personal responsibility" – all employees are called upon to handle information and IT systems responsibly and attentively in the course of their work, to identify risks and to act accordingly in order to ensure security at Scheidt & Bachmann.

Violations of this policy can result in significant reputational damage and legal disadvantages for the employees concerned, their colleagues and Scheidt & Bachmann, including fines, criminal proceedings, or restrictions on official permits. In most cases, such misconduct will also constitute a breach of employment law and may result in appropriate sanctions.

We strive to ensure that suppliers and business partners also live by and support these values and principles. Upon request and on the basis of reciprocity, contractual partners should report on the essential measures taken to comply with this policy, without however disclosing trade secrets or other information worthy of protection. Reciprocity means that the requesting party should provide information to the same extent.

This policy provides the mandatory framework for Group-wide multi-site information security and data protection management. Site- or company-specific regulations must not conflict with this policy

and are only permitted insofar as they specify or enhance local legal or regulatory requirements and have been agreed with the Chief Information Security Officer.

The Chief Information Security Officer reviews this policy annually and updates it as necessary. This policy and its updates are published and communicated in electronic form via the company-wide communication channels. Printed versions of this policy are not subject to any organised change service. The electronic form published on the company-wide channels is valid.

Mönchengladbach, 24.07.2026

Scheidt & Bachmann GmbH Management Board