

# Global Information Security and Data Protection Policy

07.07.2025

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 group of companies with regard to information security and data protection.

The Information Security and Data Protection Policy applies to the entire Scheidt & Bachmann group of companies, in particular to those Scheidt & Bachmann companies that have established an information security management system.

Scheidt & Bachmann's business activities 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 of companies 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 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,
- the integrity of the data and systems is ensured, and
- the confidentiality of processed information 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, extended by a data protection management system in accordance with DIN EN ISO/IEC 27701, in their currently valid versions. In doing so, we ensure that all requirements of these 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 system 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 information security and data protection-related performance of Scheidt & Bachmann and the ISMS;
- 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: Our goal is to have all necessary international and national Scheidt & Bachmann companies certified according to this standard by 2030.
- Training on internal ISMS guidelines: We aim to ensure that at least 90% of employees participate in mandatory training on relevant ISMS topics (e.g. data protection, information classification, or AI risks) each year. Such training helps to raise awareness and improve understanding of internal ISMS guidelines.

The Scheidt & Bachmann ISMS 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 system based on the BSI 200-4 standard is an important part of the security strategy.

The executive management and managers are responsible for integrating the contents of this policy into management decisions and for providing 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 of companies 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 designated employees and the management at the international locations who are involved in the implementation and maintenance of the ISMS, as well as the Data Protection Officer and the Chief Information Security Officer.

The Chief Information Security Officer and the Data Protection Officer of the central information security and data protection management support the Information Security Officers as designated responsible persons from the individual business units and Scheidt & Bachmann companies in which an ISMS is operated and certified in accordance with the DIN EN ISO/IEC 27001 standards (extended by DIN ISO/IEC 27701 where applicable). The Information Security Officers are supported in the

respective business units and companies by ISMS Teams. The Information Security Officers and the ISMS Team ensure that all binding obligations to the management system are implemented correctly and in an auditable manner and that the processes within this system are continuously improved.

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 shall 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.

The Chief Information Security Officer reviews this policy as necessary and proposes updates to the executive management of Scheidt & Bachmann. 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 in the company-wide channels is valid.

Mönchengladbach, 07.07.2025

Scheidt & Bachmann GmbH Management Board