

# Globale Informationssicherheits- und Datenschutz-Policy

07.07.2025

In einer zunehmend digitalisierten Welt gewinnt der Schutz von Informationen, Daten, personenbezogenen Daten und IT-Systemen immer mehr an Bedeutung. Die Sicherheit dieser Werte ist essenziell, um das Vertrauen unserer Kunden, Partner und Mitarbeitenden zu erhalten und gesetzliche sowie regulatorische Anforderungen zu erfüllen. Diese Informationssicherheits- und Datenschutz-Policy drückt die positive Haltung, das Interesse und das Verantwortungsbewusstsein der Scheidt & Bachmann Unternehmensgruppe im Hinblick auf Informationssicherheit und Datenschutz aus.

Die Informationssicherheits- und Datenschutz-Policy gilt für die gesamte Scheidt & Bachmann Unternehmensgruppe, insbesondere in den Scheidt & Bachmann Gesellschaften, die ein Informationssicherheitsmanagement etabliert haben.

Die Geschäftstätigkeit von Scheidt & Bachmann ist von der Informationstechnik mit dazugehörigen Daten und Systemen abhängig. Als global tätige Unternehmensgruppe stehen wir in der Verantwortung, die Vertraulichkeit, die Integrität und die Verfügbarkeit der in der Scheidt & Bachmann Unternehmensgruppe verarbeiteten Daten und der betriebenen Systeme zu gewährleisten und die Risiken für die Rechte und Freiheiten natürlicher Personen durch die Verarbeitung personenbezogener Daten auszuschließen. Die Einhaltung dieser Schutzziele ist für Scheidt & Bachmann von großer Bedeutung.

Für Scheidt & Bachmann ist ein hohes Maß an Informationssicherheit und Datenschutz essenziell, damit die Funktions- und Leistungsfähigkeit unserer Geschäftsprozesse sichergestellt werden. Von größter Bedeutung ist es deshalb, die Informations- und Datensicherheit auf einem angemessenen Niveau zu gewährleisten.

Die informationsverarbeitenden Systeme und die verarbeiteten Daten müssen so geschützt werden, dass

- sie und die darauf angewiesenen Geschäftsprozesse gemäß den Anforderungen verfügbar sind,
- die Integrität der Daten und Systeme sichergestellt ist und
- die Vertraulichkeit von verarbeiteten Informationen in angemessener Weise gewahrt ist.

Informationssicherheitsrisiken zu erkennen und diese durch geeignetes Handeln zu kontrollieren, d. h. auf ein angemessenes Maß zu verringern oder zu vermeiden, sehen wir als wichtige Aufgabe an. Mindestkriterien stellen hierbei die gesetzlichen und regulativen Rahmenbedingungen dar.

Unser Ziel ist es, die Informations- und Datensicherheit nicht nur auf einem risikoorientierten Niveau zu gewährleisten, sondern auch kontinuierlich zu verbessern. Um dieses Ziel zu erreichen, betreiben wir ein Informationssicherheitsmanagementsystem (ISMS) nach DIN EN ISO/IEC 27001, erweitert um

ein Datenschutzmanagementsystem nach DIN EN ISO/IEC 27701, in ihrer jeweils aktuell gültigen Fassung. Dabei tragen wir dafür Sorge, dass alle Anforderungen dieser Normen korrekt umgesetzt, die Informationssicherheits- und Datenschutzziele an den Unternehmenszielen ausgerichtet und die Prozesse und Schutzmaßnahmen innerhalb des Managementsystems kontinuierlich verbessert werden.

Scheidt & Bachmann verpflichtet sich, alle Informationen und Ressourcen bereitzustellen, die zur Erreichung der strategischen und operativen Ziele des Informationssicherheits- und Datenschutzmanagements notwendig sind. Hierfür verpflichten wir uns insbesondere

- zur kontinuierlichen Überprüfung, Bewertung und Verbesserung der informationssicherheits- und datenschutzbezogenen Leistungen von Scheidt & Bachmann und des ISMS;
- die notwendigen Ressourcen zur Erreichung der strategischen und operativen Ziele zur Verfügung zu stellen;
- das informationssicherheits- und datenschutzbewusste Handeln unserer Mitarbeitenden durch Ausbildung, Information und durch Vorbildfunktion unseres Handelns zu fördern;
- geltende gesetzliche, vertragliche und andere Anforderungen bzgl. der Informationssicherheit und des Datenschutzes einzuhalten und insbesondere hierbei die Rolle des Verantwortlichen oder des Auftragsverarbeiters zu erfüllen.

Die voran genannten Selbstverpflichtungen bilden das Fundament für die Etablierung und Aufrechterhaltung eines hohen Informationssicherheits- und Datenschutzniveaus bei Scheidt & Bachmann. Um die Wirksamkeit dieser Prinzipien sicherzustellen, streben wir in relevanten Bereichen auch messbare Fortschritte und nachweisbare Prozesse an.

Die folgenden Punkte nennen Bereiche, in denen wir uns quantitative Ziele setzen bzw. quantitative Kennzahlen erheben, um die Einhaltung unserer Grundsätze zu fördern und zu überwachen:

- Erweiterung des DIN EN ISO/IEC 27001 Geltungsbereiches: Unser Ziel ist es, bis 2030 alle erforderlichen internationalen und nationalen Scheidt & Bachmann Gesellschaften nach diesem Standard zertifizieren zu lassen.
- Schulung interner ISMS-Richtlinien: Wir setzen uns als Ziel, dass jährlich mind. 90% der Mitarbeitenden an verpflichtenden Schulungen zu relevanten ISMS-Themen teilnehmen (z. B. Datenschutz, Informationsklassifizierung oder KI-Risiken). Solche Schulungen tragen zur Sensibilisierung und zum besseren Verständnis interner ISMS-Richtlinien bei.

Das Scheidt & Bachmann ISMS-Handbuch sowie weiterführende Dokumente und Prozesse spezifizieren das Informationssicherheits- und Datenschutzmanagement und haben verbindliche Geltung für alle Mitarbeitenden von Scheidt & Bachmann.

Zur Aufrechterhaltung und Wiederherstellung der Geschäftsprozesse im Fall von Sicherheitsvorfällen, Katastrophen oder anderen Störungen ist der Aufbau eines Business Continuity Management in Anlehnung an den BSI 200-4 Standard ein wichtiger Bestandteil der Sicherheitsstrategie.

Die Geschäftsführung und Führungskräfte sind verantwortlich für die Integration der Inhalte dieser Policy in Managemententscheidungen und für die Bereitstellung der notwendigen Ressourcen. Alle Mitarbeitenden, einschließlich der Geschäftsführung und der Führungskräfte mit ihrer Vorbildfunktion, sind für die Einhaltung dieser Policy verantwortlich.

Verantwortlich für die Erreichung unserer Ziele sind alle Fachbereiche der Scheidt & Bachmann Unternehmensgruppe, deren Handeln maßgeblichen Einfluss auf die Zielerreichung hat. Für die

genannten quantitativen Ziele sind das die Mitarbeitenden des IT Infrastructure & Client IT Services Bereichs, die Information Security Officer, die benannten Mitarbeitenden sowie das Management in den internationalen Standorten, die an der Implementierung und Aufrechterhaltung des ISMS mitwirken, sowie die Datenschutzbeauftragte als auch der Chief Information Security Officer.

Der Chief Information Security Officer sowie die Datenschutzbeauftragte des zentralen Informationssicherheits- und Datenschutzmanagements unterstützen die Information Security Officer als benannte Verantwortliche aus den einzelnen Geschäftsbereichen und Scheidt & Bachmann Gesellschaften, in denen ein ISMS nach den Normen DIN EN ISO/IEC 27001 (ggf. erweitert um DIN ISO/IEC 27701) betrieben und zertifiziert wird. Die Information Security Officer werden in den jeweiligen Geschäftsbereichen und Gesellschaften durch zusammengestellte ISMS-Teams unterstützt. Die Information Security Officer und das ISMS-Team tragen dafür Sorge, dass alle bindenden Verpflichtungen an das Managementsystem korrekt und auditierbar umgesetzt werden, und dass die Prozesse innerhalb dieses Systems kontinuierlich verbessert werden.

Im Sinne unserer Unternehmenswerte – insbesondere des Wertes „Vertrauen & Selbstverantwortung“ – sind alle Mitarbeitenden aufgerufen, im Rahmen ihrer Tätigkeit verantwortungsbewusst und aufmerksam mit Informationen und IT-Systemen umzugehen, Risiken zu erkennen und entsprechend zu handeln, um die Sicherheit bei Scheidt & Bachmann zu gewährleisten.

Verstöße gegen diese Policy können erhebliche Reputationsverluste und rechtliche Nachteile für die betreffenden Mitarbeitenden, deren Kolleg\*innen und Scheidt & Bachmann zur Folge haben, bis hin zu Bußgeldern, Strafverfahren oder Einschränkungen behördlicher Erlaubnisse. Zumeist wird ein solches Fehlverhalten dann auch eine arbeitsrechtliche Pflichtverletzung sein und zu entsprechenden Sanktionen führen können.

Es wird angestrebt, dass Lieferanten und Geschäftspartner die Werte und Grundsätze ebenfalls leben und unterstützen. Auf Verlangen und im Rahmen von Reziprozität sollen Vertragspartner über die wesentlichen Maßnahmen zur Einhaltung dieser Policy berichten, jedoch ohne Offenlegung von Geschäftsgeheimnissen oder sonst schützenswerten Informationen. Reziprozität bedeutet, dass der Anfragende im gleichen Umfang Informationen zur Verfügung stellen sollte.

Der Chief Information Security Officer überprüft diese Policy bei Bedarf und schlägt der Geschäftsführung von Scheidt & Bachmann eine Aktualisierung vor. Diese Policy und ihre Aktualisierungen werden in unternehmensweiten Kommunikationskanälen in elektronischer Form publiziert und kommuniziert. Ausgedruckte Versionen dieser Policy unterliegen keinem organisierten Änderungsdienst. Gültig ist die jeweils in den unternehmensweiten Kanälen publizierte elektronische Form.

Mönchengladbach, den 07.07.2025

Die Geschäftsführung der Scheidt & Bachmann GmbH