Globale Informationssicherheits- und Datenschutz-Policy

24.07.2026

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 Informationssicherheits- und Datenschutzmanagement etabliert haben. Die Managementsysteme werden jeweils als zentrales Multi-Site-Managementsystem betrieben und umfassen alle Scheidt & Bachmann Gesellschaften und Standorte, die in den definierten Anwendungsbereich des jeweiligen Managementsystems aufgenommen sind oder aufgenommen werden.

Die Geschäftstätigkeit von Scheidt & Bachmann ist wesentlich von der Informationstechnologie sowie den zugehörigen 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 Informationen bzw. Daten müssen so geschützt werden, dass

- sie und die darauf angewiesenen Geschäftsprozesse gemäß den Anforderungen verfügbar sind,
- ihre Integrität sichergestellt ist und
- die Vertraulichkeit 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 regulatorischen 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 27001:2024, sowie ein Datenschutzmanagementsystem (PIMS) nach DIN EN ISO/IEC 27701:2026, in ihrer jeweils aktuell gültigen Fassung. Das ISMS und PIMS sind als zertifizierte Multi-Site-Managementsysteme ausgestaltet. Im Rahmen beider Managementsysteme werden zentrale Vorgaben durch lokal verantwortliche Organisationseinheiten und Standorte umgesetzt, überwacht und kontinuierlich verbessert. Dabei tragen wir dafür Sorge, dass alle Anforderungen der Normen korrekt umgesetzt, die Informationssicherheits- und Datenschutzziele an den Unternehmenszielen ausgerichtet und die Prozesse und Schutzmaßnahmen innerhalb der Managementsysteme 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, des ISMS und des PIMS;
- 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 27001:2024 Anwendungsbereiches: Bis zum 31.12.2030 sollen 100 % der im Zertifizierungsprogramm definierten Scheidt & Bachmann Gesellschaften nach DIN EN ISO/IEC 27001:2024 zertifiziert sein. Die Zielerreichung wird anhand des Anteils zertifizierter Gesellschaften jährlich gemessen und im ISMS Management Review bewertet. Der Zertifizierungsumfang wird jährlich überprüft und fortgeschrieben.
- Schulungen interner ISMS- und PIMS-Richtlinien: Bis zum 31.12.2027 sollen mindestens 90 % der Mitarbeitenden an den verpflichtenden Schulungen zu relevanten ISMS- und PIMS-Themen teilgenommen haben. Die Zielerreichung wird anhand der Schulungsquote jährlich gemessen und im Management Review bewertet. Die erreichte Teilnahmequote wird anschließend dauerhaft aufrechterhalten und jährlich überprüft.

Das Scheidt & Bachmann ISMS- bzw. PIMS-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 internationale Standards (z. B. ISO 22301, BSI 200-4) ein wichtiger Bestandteil der Sicherheitsstrategie.

Die Oberste Leitung (Group CEO) trägt die Gesamtverantwortung für das gruppenweite ISMS bzw. PIMS und für das Einhalten der Anforderungen an die Informationssicherheit.

Für die strategische und operative Umsetzung des ISMS ist ein Chief Information Security Officer bestellt, der die Gesamtverantwortung für die Informationssicherheit der Scheidt & Bachmann Unternehmensgruppe trägt.

Für die strategische und operative Umsetzung des PIMS sowie für den Datenschutz innerhalb der Scheidt & Bachmann Unternehmensgruppe ist die bestellte Datenschutzbeauftragte der Scheidt & Bachmann GmbH zuständig.

Die Geschäftsführung sowie die Führungskräfte der einzelnen Gesellschaften und Standorte sind verantwortlich für die standortspezifische Umsetzung dieser Policy sowie daraus abgeleitete Richtlinien, Prozesse, Verfahren, Standards, Konzepte und Maßnahmen, und stellen dafür die notwendigen Ressourcen bereit. 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 Datenschutzkoordinatoren, die benannten Mitarbeitenden sowie das Management in den nationalen/internationalen Standorten, die an der Implementierung und Aufrechterhaltung des ISMS bzw. des PIMS mitwirken, sowie die Datenschutzbeauftragte als auch der Chief Information Security Officer.

Die benannten Information Security Officer der einzelnen Geschäftsbereiche und Gesellschaften übernehmen die Rolle der lokalen Verantwortlichen innerhalb des Multi-Site-ISMS. Sie stellen sicher, dass die zentral definierten Anforderungen des ISMS an ihrem jeweiligen Standort vollständig, wirksam und auditierbar umgesetzt werden. Die Information Security Officer werden in den jeweiligen Geschäftsbereichen und Gesellschaften durch den Chief Information Security Officer sowie durch die jeweils zusammengestellten ISMS-Teams unterstützt.

Die benannten Datenschutzkoordinatoren der einzelnen Geschäftsbereiche und Gesellschaften übernehmen die Rolle der lokalen Verantwortlichen innerhalb des Multi-Site-PIMS. Sie stellen sicher, dass die zentral definierten Anforderungen des PIMS an ihrem jeweiligen Standort vollständig, wirksam und auditierbar umgesetzt werden. Die Datenschutzkoordinatoren werden in den jeweiligen Geschäftsbereichen und Gesellschaften durch die Datenschutzbeauftragte sowie durch die jeweils zusammengestellten PIMS-Teams unterstützt.

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.

Diese Policy bildet den verbindlichen Rahmen für das jeweils gruppenweite Multi-Site-Informationssicherheits- und Datenschutzmanagement. Standort- oder gesellschaftsspezifische Regelungen dürfen dieser Policy nicht widersprechen und sind ausschließlich zulässig, soweit sie lokale rechtliche oder regulatorische Anforderungen konkretisieren oder verschärfen und mit dem Chief Information Security Officer abgestimmt sind.

Der Chief Information Security Officer überprüft diese Policy jährlich und passt sie bei Bedarf an. 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 24.07.2026

Die Geschäftsführung der Scheidt & Bachmann GmbH