

1 Anwendungsbereich

Die Informationssicherheitspolitik gilt für alle Bereiche im Scope des Informationssicherheitsmanagementsystems (ISMS) der Thieme Gruppe.

Die Informationssicherheitspolitik dient als strategischer Leitfaden zur Sicherstellung der Sicherheit und Resilienz von Informationen bei Thieme.

2 Unternehmen und Geschäftszweck

Die Thieme Gruppe ist ein international tätiges Medien- und Dienstleistungsunternehmen mit Schwerpunkt auf Medizin und Gesundheitswesen. Seit 1886 steht das Familienunternehmen für Medizinkompetenz und Gesundheitsexpertise. Durch eine enge Vernetzung mit sämtlichen Leistungserbringern des Gesundheitswesens und direkten Zugang zu Experten aus Medizin und Wissenschaft entwickelt Thieme neben klassischen Verlagsprodukten innovative E-Health-Lösungen und unterstützt die evidenzbasierte Medizin durch hochwertige Inhalte und Dienstleistungen.

Alle geschäftlichen Aktivitäten der Thieme Gruppe orientieren sich an unserer Vision **"Für eine bessere Medizin und mehr Gesundheit im Leben"**. Dieses Ziel möchten wir mit unserer Mission **"Mit den entscheidenden Informationen zur richtigen Zeit am richtigen Ort"** erreichen.

3 Bedeutung der Sicherheit

Die Informationssicherheit gewinnt für unsere Kunden zunehmend an Bedeutung, da Geschäfts- und Behandlungsprozesse immer stärker von den richtigen Informationen und von IT-Systemen abhängig sind. Unsere Kunden und deren Patienten erwarten von uns als Anbieter von Systemlösungen die Erfüllung höchster Sicherheitsanforderungen.

Als Anbieter cloudbasierter Software-Services für das Gesundheitswesen trägt die Thieme Gruppe besondere Verantwortung für den Schutz der verarbeiteten Informationen. Kunden unserer Cloud-Dienste vertrauen auf die sichere Verarbeitung, Speicherung und Bereitstellung ihrer Daten und erwarten die Wahrung von Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der bereitgestellten Services. Die Informationssicherheit ist daher eine wesentliche Voraussetzung für die Erfüllung vertraglicher Kundenanforderungen sowie gesetzlicher und regulatorischer Verpflichtungen.

Das Vertrauen in die Qualität und Sicherheit unserer Services und Produkte ist ein zentrales Gut der Thieme Gruppe und steht in direktem Zusammenhang mit unserem Geschäftserfolg.

Vor diesem Hintergrund ist die Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur. Jeder Mitarbeitende ist sich der Bedeutung der Informationssicherheit bewusst und kennt die möglichen Auswirkungen von Risiken auf den Geschäftserfolg der Thieme Gruppe.

4 Informationssicherheitsmanagementsystem

Um diesen Anforderungen gerecht zu werden betreibt die Thieme Gruppe ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheitsmanagementsystem (ISMS) mit dem Geltungsbereich **Bereitstellung, Wartung und Weiterentwicklung der IT-Infrastruktur, einschließlich Rechenzentrum, Netzwerk, Speicher, physischer Server und Virtualisierung, die Erbringung der IT-Client-Services sowie die Softwareentwicklung, Bereitstellung, Inbetriebnahme und den technischen Support der Produktfamilien E-Consent Pro (ECP) und Thieme Flow sowie den Betrieb der cloudbasierten Software-Services E-Consent Pro Patient und Thieme Flow. Darüber hinaus umfasst der Geltungsbereich die Bereitstellung und den Betrieb digitaler und hybrider telemedizinischer Gesundheitsservices.**

Der Geltungsbereich umfasst folgende Standorte:

Georg Thieme Verlag KG Oswald-Hesse-Straße 50 70469 Stuttgart	Steuerung ISMS, Bereitstellung, Wartung und Weiterentwicklung der IT-Infrastruktur mit den Bereichen Rechenzentrum, Netzwerk und Speicher, Physische Server und Virtualisierung, Erbringung der IT-Client-Services
Thieme Compliance GmbH Am Weichselgarten 30a 91058 Erlangen	Softwareentwicklung, Bereitstellung, Inbetriebnahme und den technische Support der Produktfamilien E-Consent Pro (ECP) und Thieme Flow sowie den Betrieb der cloudbasierten Software-Services E-Consent Pro Patient und Thieme Flow
Thieme Telecare GmbH Oswald-Hesse-Straße 50 70469 Stuttgart	Bereitstellung und Betrieb digitaler und hybrider telemedizinischer Gesundheitsservices.

Die Thieme Gruppe stellt die Wirksamkeit und kontinuierliche Verbesserung ihres Informationssicherheitsmanagementsystems durch die Anwendung des Plan-Do-Check-Act-Modells (PDCA) sicher.

- Plan: Festlegung von Sicherheitszielen, Bewertung von Risiken und Chancen sowie Planung geeigneter Maßnahmen zur Erreichung der Sicherheitsziele.
- Do: Umsetzung und Betrieb der festgelegten organisatorischen, technischen und prozessualen Maßnahmen.
- Check: Regelmäßige Überwachung, Messung und Bewertung der Wirksamkeit des ISMS, insbesondere durch Risikobewertungen, interne Audits, Kontrollaktivitäten und Managementbewertungen.
- Act: Ableitung und Umsetzung von Korrektur-, Verbesserungs- und Optimierungsmaßnahmen zur kontinuierlichen Weiterentwicklung des ISMS.

Durch diesen systematischen Ansatz wird sichergestellt, dass die Informationssicherheit dauerhaft aufrechterhalten, regelmäßig überprüft und fortlaufend an neue Anforderungen, Risiken und Rahmenbedingungen angepasst wird.

Zusätzlich implementiert und betreibt Thieme für die cloudbasierten Software-Services E-Consent Pro Patient und Thieme Flow ein Internes Kontrollsystem (IKS) gemäß den Anforderungen des BSI C5. Das IKS ergänzt die im ISMS etablierten Steuerungs- und Verbesserungsprozesse und stellt sicher, dass die definierten Sicherheitsziele und Kontrollmechanismen regelmäßig überprüft, dokumentiert und kontinuierlich verbessert werden.

5 Ziele der Informationssicherheit

Die Thieme Gruppe verfolgt klare und übergeordnete Ziele zur Informationssicherheit. Diese bilden die Grundlage für alle organisatorischen, technischen und prozessualen Maßnahmen im Rahmen des Informationssicherheitsmanagementsystems (ISMS).

Ziel der Informationssicherheit ist es insbesondere:

- die **Vertraulichkeit** von Informationen und Daten zu wahren,
- die **Integrität und Authentizität** von Informationen, Daten, Prozessen, IT-Anwendungen und Systemen sicherzustellen,
- die **Verfügbarkeit** von Informationen und Systemen zur richtigen Zeit und am richtigen Ort zu gewährleisten.

6 Grundsätzliche Regelungen

Unsere Sicherheitsstrategie verfolgt einen risikobasierten Ansatz, setzt auf kontinuierliche Verbesserung und umfasst ein strukturiertes Notfallmanagement. Darüber hinaus werden technische und organisatorische Maßnahmen implementiert, um die definierten Sicherheitsziele nachhaltig zu erreichen.

Die folgenden grundsätzlichen Regelungen bilden die organisatorischen und prozessualen Rahmenbedingungen für die Umsetzung und Aufrechterhaltung der Informationssicherheit:

- **Governance und Verantwortung:** Die Thieme Gruppe betreibt ein Informationssicherheitsmanagementsystem (ISMS), das durch die Konzernleitung gesteuert wird. Hierzu wurde ein Information Security Board (ISB) unter Vorsitz des CTO eingerichtet. Der Information Security Management Officer (ISMO) ist Mitglied des ISB und verantwortet die Security Governance, einschließlich Richtlinien, Prozesse, Sensibilisierung und Überwachung der Einhaltung. Er berichtet regelmäßig im ISB über den Status des ISMS, Ergebnisse von Audits und Risikobewertungen sowie über Verbesserungsmaßnahmen.
- **Richtlinien und Mitarbeitendenverantwortung:** Die Informationssicherheit wird durch operative Sicherheitsrichtlinien geregelt. Alle Mitarbeitenden sind verpflichtet, diese einzuhalten und verantwortungsvoll mit Daten und Informationen umzugehen.
- **Risikomanagement und Schutzmaßnahmen:** Relevante Informationen, Systeme und Prozesse werden identifiziert, regelmäßig risikobewertet und bei Änderungen aktualisiert. Auf Basis der Risikobewertungen werden geeignete technische und organisatorische Maßnahmen zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität umgesetzt.
- **Zugriffs- und Berechtigungsmanagement:** Der Zugang zu sensiblen Systemen, Sicherheitszonen und kritischen Informationen ist durch geeignete technische, organisatorische und infrastrukturelle Maßnahmen geschützt und erfolgt ausschließlich über formalisierte Vergabe- und Entzugsverfahren.
- **Awareness und Schulungen:** Alle Mitarbeitenden werden regelmäßig durch Schulungen und Sensibilisierungsmaßnahmen zu Informationssicherheit und Datenschutz geschult, um ein hohes Sicherheitsbewusstsein im gesamten Unternehmen sicherzustellen.
- **Nachweisführung und Dokumentation:** Die Umsetzung der Informationssicherheit wird dokumentiert und durch ein geregeltes Dokumentenmanagement unterstützt.

7 Führung und Verpflichtung der Geschäftsführung

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Geschäftsführung der Thieme Gruppe. Sie unterstützt aktiv die Sicherheitsorganisation und stellt sicher, dass das Informationssicherheitsmanagementsystem (ISMS) wirksam implementiert, betrieben, überwacht und kontinuierlich verbessert wird.

Die Geschäftsführung verpflichtet sich insbesondere zu folgenden Grundsätzen:

- **Strategische Verankerung und Governance:** Die Informationssicherheitspolitik und die Informationssicherheitsziele sind festgelegt und mit der strategischen Ausrichtung der Organisation abgestimmt. Die Geschäftsführung stellt sicher, dass das ISMS seine beabsichtigten Ergebnisse erzielt und wirksam gesteuert wird.
- **Ressourcen, Verantwortung und Führung:** Die für den Betrieb und die Weiterentwicklung des ISMS erforderlichen Ressourcen werden bereitgestellt. Führungskräfte werden angeleitet und unterstützt, ihre Verantwortung für Informationssicherheit in ihren jeweiligen Bereichen wahrzunehmen.
- **Wirksamkeit und kontinuierliche Verbesserung:** Die Bedeutung eines wirksamen Informationssicherheitsmanagements wird organisationweit vermittelt. Die Geschäftsführung fördert die aktive Beteiligung aller Mitarbeitenden und wendet das Prinzip der kontinuierlichen Verbesserung an.

- **Einhaltung von Normen und regulatorischen Anforderungen:** Die Thieme Gruppe betreibt ihr ISMS nach ISO/IEC 27001. Für die nach BSI C5 geprüften Cloud-Dienste werden zusätzlich die entsprechenden Anforderungen des BSI C5 umgesetzt. Die Umsetzung der entsprechenden Kontrollen und Maßnahmen wird regelmäßig überprüft, dokumentiert und weiterentwickelt.

8 Kommunikation der Informationssicherheitspolitik

Diese Informationssicherheitspolitik ist allen Mitarbeitenden im Geltungsbereich des Informationssicherheitsmanagementsystems bekannt und dauerhaft zugänglich. Darüber hinaus wird sie relevanten externen Parteien, insbesondere Auftragnehmern sowie Kunden der im Geltungsbereich enthaltenen Cloud-Dienste, zur Verfügung gestellt.