KENNZEICHNUNG	**ÖFFENTLICH**
Version	2.0
Datum	14.04.2026

Information Security Policy

SICHERHEITSPOLITIK DER **IMENDO GmbH.**

1. Leitbild

Als einer der führenden, eigentümergeführten IT-Dienstleister im deutschsprachigen Raum gestalten wir seit 2010 die digitale Zukunft unserer Kund:innen. Imendo steht für individuelle IT-Lösungen, die unsere Kunden nachhaltig erfolgreicher machen. Mit Erfahrung, technologischem Weitblick und partnerschaftlicher Zusammenarbeit verwandeln wir Daten in Wettbewerbsvorteile, optimieren Abläufe und gestalten moderne Arbeitswelten, damit unsere Kunden ihr volles Potenzial entfalten können. Unsere Vision ist es, der verlässlichste Partner für unsere Kunden bei der digitalen Transformation zu sein und durch innovative IT-Lösungen rund um Data, KI und moderne Arbeitswelten nachhaltigen Erfolg und positive Veränderungen zu schaffen.

Wir nutzen modernste Informations- und Kommunikationstechnologien und -prozesse, um dies zu erreichen und so einen effizienten, qualitativ hochwertigen und termingerechten internen Betrieb sowie die termingerechte Lieferung an unsere Kunden sicherzustellen. Da wir die entscheidende Bedeutung einer sicheren und ständig verfügbaren Informationsverarbeitung anerkennen, hat die Informationssicherheit bei IMENDO höchste Priorität. Technische Störungen, Fehlverhalten, Sabotage und Spionage können die Funktionalität und Verfügbarkeit unserer IT-Systeme und -Netzwerke sowie die Vertraulichkeit und Integrität unserer Geschäftsprozesse und Daten erheblich gefährden. Im schlimmsten Fall könnte dies unserem Ruf schaden und zu finanziellen Verlusten sowie potenziellen Umwelt- und Gesundheitsrisiken führen.

Um diese Risiken zu minimieren, haben wir ein integriertes Informationssicherheitsmanagementsystem (ISMS) eingerichtet, das Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität nachhaltig und kosteneffektiv schützt.

1.1 Stellenwert der Informationsverarbeitung und Sicherheit

Die Führung der Imendo GmbH bekennt sich zu dem Wert und dem daraus abgeleiteten Schutzbedarf der in der Imendo GmbH verarbeiteten Informationen. Der Verlust, Diebstahl, Manipulation oder Nicht Auffindbarkeit dieser Informationen kann einen Schaden für die IMENDO GmbH bedeuten – die Palette reicht von geringfügig bis existenzbedrohend.

Die Aufgabenerfüllung innerhalb der IMENDO GmbH ist abhängig von ordnungsgemäßer und datenschutzkonformer Verarbeitung von Informationen.

Die einzelnen Geschäftsbereiche sind durch die Einhaltung der Informationssicherheitsleitlinie dazu verpflichtet sich um einen angemessenen Schutz der Informationen gemäß ihrer Wertigkeit und ihres Risikos für das jeweilige Geschäftsfeld oder das technische Umfeld zu kümmern.

1.2 Ziele der Informationssicherheit

Ziel der Informationssicherheit ist die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Die Informationssicherheit muss in allen Projekten und fachlichen Verfahren beachtet und integriert werden. Alle Sicherheitsmaßnahmen müssen in Einklang mit den Sicherheitszielen, der IT-Strategie und den Informationssicherheitsrichtlinien sein sowie den Zielen der Imendo GmbH entsprechen. Die geforderten Sicherheitsmaßnahmen sollen im wirtschaftlich vertretbaren Rahmen und Verhältnis zu den schützenden Informationen und Werten des Unternehmens stehen.

Folgende allgemeingültigen Sicherheitsziele werden definiert:

- Einsatz modernster Methoden zur Sicherung unserer Dienste, Einrichtungen, Daten und Informationen zur Verhinderung unbefugten Zugriffs oder Diebstahls.
- Einhaltung der gesetzlichen Vorgaben und Umsetzung der daraus resultierenden Anforderungen an die Informationssicherheit, Gewährleistung der Einhaltung des österreichischen Datenschutzgesetzes DSG bei der Verarbeitung personenbezogener Daten
- Regelmäßige Bewertung der Risiken neuer Technologien und Integration der Informationssicherheit in unsere Entscheidungsprozesse für Beschaffung und Betrieb, wobei Wert auf Effizienz und Benutzerfreundlichkeit gelegt wird.
- Kontinuierliche Verbesserung und Aktualisierung der Sicherheitsmaßnahmen, um uns an die sich wandelnde Bedrohungslandschaft anzupassen und potenziellen Risiken und Schwachstellen einen Schritt voraus zu sein.
- Regelmäßige Schulungen und Sensibilisierungsprogramme für alle Mitarbeitenden, um ein sicherheitsbewusstes Denken zu fördern und sie zu befähigen, potenzielle Sicherheitsvorfälle zu erkennen und zu verhindern.
- Zuverlässige Unterstützung der Geschäftsprozesse und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb des Unternehmens.
- Etablierung eines transparenten und effizienten Notfallplans, um Sicherheitsverletzungen schnell zu identifizieren, einzudämmen und zu beheben und so deren Auswirkungen zu minimieren und zukünftige Vorfälle zu verhindern

1.3 Informationssicherheitsstrategie

Unsere Ziele werden durch die Umsetzung folgender Punkte erreicht:

- Ein Informationssicherheitsmanagementsystem (ISMS) wurde auf Basis international anerkannter Standards eingerichtet.
- Unser Team hat ein Schulungs- und Sensibilisierungsprogramm entwickelt, um alle Mitarbeitenden über die neuesten technischen Kenntnisse und Best Practices im Bereich Informationssicherheit auf dem Laufenden zu halten.
- Messbare Informationssicherheitsziele und Prüfmaßnahmen wurden eingeführt, um die Effektivität und Qualität unseres ISMS und unserer operativen Maßnahmen kontinuierlich zu bewerten und zu verbessern.
- Wir haben Prozesse für die gesetzlich vorgeschriebene Kommunikation mit Behörden und Kunden im Falle von Sicherheitsvorfällen oder Anfragen im Zusammenhang mit personenbezogenen Daten und Informationen eingerichtet.

2. Geltungsbereich, Integration im Unternehmen

Unsere Informationssicherheitsrichtlinie gilt für die gesamte IMENDO GmbH, für beide Standorte Klagenfurt und Wien. Sie umfasst alles, was wir tun, einschließlich Prozesse, Vermögenswerte und Informationen, die alle für das Erreichen unserer Unternehmensziele wichtig sind.

Wir verpflichten alle Auftragnehmer, diese Richtlinie zu kennen und einzuhalten, insbesondere beim Kauf neuer IT-Systeme. Wir stellen dies sicher, indem wir die relevanten Vorschriften in unsere Einkaufsbedingungen und Planungsdokumente aufnehmen. Wir können diese Richtlinie auch als Referenz bei der Erstellung von Einzelverträgen verwenden. Alle unsere Mitarbeiter müssen die festgelegten Grundsätze und Standards beim Umgang mit Informationswerten befolgen. Dies umfasst die Planung, Entwicklung, Beschaffung, Einrichtung, den Betrieb und die Entsorgung dieser Werte.

3. Grundsätze

Unser Informationssicherheitsmanagementsystem ist gemäß ISO/IEC 27001:2022 und anderen anerkannten Standards und Rahmenwerken konzipiert und wird kontinuierlich verbessert. Dabei berücksichtigen wir folgende Kernprinzipien:

- Die Ziele der Informationssicherheit sind auf die Gesamtziele der IMENDO GmbH abgestimmt und fördern unternehmensweit eine Kultur des Sicherheitsbewusstseins und der entsprechenden Verantwortung.
- Die Maßnahmen zur Informationssicherheit und die Risikomanagementprozesse leiten sich aus unserer Informationssicherheitsrichtlinie ab, um sicherzustellen, dass sie dem jeweiligen Bedrohungsniveau angemessen sind.
- Wir nutzen grundlegende Schutzmaßnahmen und detaillierte Risikoanalysen, um ein risikoadaptives Sicherheitsniveau zu erreichen.
- Wir wählen und implementieren Informationssicherheitsmaßnahmen risikobasiert und unter Berücksichtigung des aktuellen Stands der Technik. Diese Maßnahmen werden im Rahmen unseres kontinuierlichen Innovationsprozesses regelmäßig überprüft und aktualisiert.
- Mitarbeiter erhalten nur die für ihre Aufgaben notwendigen Informationen. Technische und organisatorische Maßnahmen verhindern eine Informationsüberflutung. Der Zugriff erfolgt nach dem Prinzip „Need-to-know“ und „Least Privilege“. Wir trennen unvereinbare Funktionen, Rollen und Verantwortlichkeiten, um Fehler und Manipulationen zu vermeiden. Ist eine funktionale Trennung nicht möglich, setzen wir genehmigte Ausgleichsmaßnahmen um.
- Gemäß unserer Informationssicherheitsrichtlinie protokollieren wir alle Informationszugriffe und stellen sicher, dass diese ausschließlich im Rahmen der zugewiesenen Aufgaben erfolgen.
- Audits und regelmäßige Risikoanalysen bewerten die Einhaltung der Prinzipien und die Effektivität unseres Informationssicherheitsmanagementsystems. Wir dokumentieren die Ergebnisse und entwickeln darauf basierend spezifische Maßnahmen.
- Daten und Informationen werden nach Vertraulichkeit, Integrität, Verfügbarkeit und datenschutzrechtlicher Relevanz klassifiziert.
- Wir bieten unseren Mitarbeitern regelmäßig Schulungen und Sensibilisierungsmaßnahmen an, um einen verantwortungsvollen Umgang mit Informationen zu fördern. Dazu gehört auch die Schulung zur Erkennung von Bedrohungen wie Phishing und Social Engineering.
- Es sind Prozesse für das Incident-Management implementiert, um Sicherheitsvorfälle zu identifizieren, zu bewerten und darauf zu reagieren. Dies gewährleistet eine zeitnahe Kommunikation und Behebung.
- Alle Informationswerte werden identifiziert, klassifiziert und einem Verantwortlichen zugewiesen, um einen angemessenen Schutz sicherzustellen.
- Externe Dienstleister und Partner werden sorgfältig geprüft, um sicherzustellen, dass sie unsere Informationssicherheitsstandards erfüllen und sich dem Datenschutz gleichermaßen verpflichtet haben.
- Notfall- und Wiederherstellungspläne werden regelmäßig entwickelt, getestet und aktualisiert, um die Auswirkungen potenzieller Störungen zu minimieren und die schnelle Wiederherstellung des Betriebs zu gewährleisten.
- Die kontinuierliche Überwachung und Verbesserung unseres Informationssicherheitsmanagementsystems erfolgen durch die Erfassung und Analyse relevanter Kennzahlen. Diese Kennzahlen dienen als Grundlage für Entscheidungen und helfen uns, Verbesserungspotenziale zu identifizieren.

4. Erreichen dieser Ziele

Informationssicherheit entsteht nicht von selbst aus Technik oder Know-how, sondern zunächst aus dem Bewusstsein des Managements und der MitarbeiterInnen einer Organisation, dass Informationen schützenswerte und gefährdete Werte für alle Beteiligten darstellen. Daher sind auch kontinuierlich Anstrengungen und Kosten für Informationssicherheit in Kauf zu nehmen, um sie zu erhalten. Zu diesem Zweck verpflichtet sich die Führung der IMENDO GmbH auch dafür zu sorgen, dass das Informationssicherheitsmanagementsystem stetig verbessert wird. Es ist

aber auch bei der Informationssicherheit nicht sinnvoll, über das Ziel hinauszuschießen: 100 % Sicherheit ist nicht erreichbar, wie viel man auch investiert.

Zur Verantwortung der Managementebene gehört neben der Erreichung der geschäftlichen wie unternehmenspolitischen Ziele auch der angemessene Umgang mit Risiken. Sie müssen so früh wie möglich erkannt, eingeschätzt, bewertet und durch Setzen geeigneter und nachhaltiger Maßnahmen auf einen minimalen und akzeptierten Rest reduziert werden. Wegen der immer höheren Abhängigkeit von Informationen gilt dies besonders für Risiken aus fehlender oder mangelhafter Informationssicherheit.

Die Führung der Imendo GmbH stellen jene Ressourcen bereit, um die entsprechend der Risikobewertung abgeleiteten Maßnahmen auch umsetzen zu können und bekennt sich zur vollumfänglichen Einhaltung der Vorgaben aus der Norm ISO-27001.

5. Durchsetzung und Sanktionen

Die Geschäftsleitung der IMENDO GmbH stellt sicher, dass angemessene Informationssicherheitsmaßnahmen implementiert werden. Wir überwachen aktiv die Einhaltung dieser Sicherheitsmaßnahmen. Sollten Mitarbeiter diese nicht einhalten, weist die Geschäftsleitung sie auf ihre Pflichten hin. Bei Bedarf werden Verstöße gemäß den internen Personalrichtlinien der IMENDO GmbH und dem geltenden österreichischen Arbeitsrecht geahndet.

6. Verbindliche Verpflichtungserklärung

Der Geschäftsführer und der Informationssicherheitsbeauftragte der IMENDO GmbH haben diese Informationssicherheitsrichtlinie, Version 2.0, mit Wirkung zum 14.04.2026 erstellt. Diese Richtlinie bildet die Grundlage für alle IT-bezogenen Entscheidungen und Maßnahmen im Unternehmen. Sie ist auf unsere übergeordneten Unternehmensstrategien abgestimmt und entscheidend für das Erreichen unserer Geschäftsziele und die Umsetzung unserer IT-Strategie. Die IMENDO GmbH verpflichtet sich zur Implementierung, Aufrechterhaltung und kontinuierlichen Verbesserung dieser Informationssicherheitsrichtlinie.

Ab dem 14.04.2026 sind die Informationssicherheitsrichtlinie, die zugehörigen Standards, Richtlinien und Arbeitsanweisungen für alle Mitarbeiter der IMENDO GmbH verbindlich. Diese Richtlinie gilt auch für externe Dienstleistungspartner und Mitarbeiter des Unternehmens.

7. Leistung und Überprüfung

Diese Richtlinie wird mindestens jährlich oder bei wesentlichen organisatorischen Änderungen überprüft. Die Leistung wird durch interne Audits, Managementbewertungen und die Überwachung wichtiger Sicherheitskennzahlen gemessen.

imendo	**Unterzeichner**	Dr. Jörg Kerschbaumer
	Datum/Zeit-UTC	2026-04-13T07:55:58+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	