Informationssicherheits-leitlinie

ISO 27001:2022

Inworks GmbH
Hörvelsinger Weg 39
89081 Ulm

Version	2
Revision / Stand	06.02.2025
Status	Freigegeben
Verantwortlicher (ISK)	Tobias Wintergerst
Empfängerkreis	Alle Beschäftigten

Änderungsverzeichnis:

Version, Datum	Änderung
Version 2, 06.02.2025	Konkretisierung der Ziele und Verpflichtung intern.

Inhaltsverzeichnis

1. Einleitung

Diese Leitlinie zur Informationssicherheit beschreibt die Anforderungen und Ziele im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb des Anwendungsbereichs des ISMS.

Das Informationssicherheitsmanagementsystem beruht auf der ISO/IEC 27001. In diesem Rahmen wird auch der Datenschutz nach BDSG und der DSGVO betrachtet. Gemeinsam bilden sie das Informationssicherheitsmanagementsystem (ISMS).

2. Unternehmen und Zweck

Die Inworks GmbH ist Hersteller der Softwarelösungen Inquery und Intrafox mit Fokus auf den Health Care Bereich. Wir digitalisieren unter anderem die Themen der Patientensicherheit und Compliance sowie des Qualitäts-, Risiko- und Feedbackmanagements: Z.B. Beschwerden, Risiken, Audits, 360-Grad-Feedback oder das Feedback von Mitarbeitern und Patienten.

Im Rahmen unserer Aufgaben und Pflichten gegenüber Kunden, Partnern, Beschäftigten und sonstigen Dritten erheben, verarbeiten und nutzen wir auch Daten und Informationen, die einen definierten Schutzbedarf aufweisen. Daher sind der Schutz und die Sicherung dieser Informationen vor der unberechtigten Kenntnisnahme durch nicht authentifizierte Personen von entscheidender Bedeutung.

Wir als Geschäftsführung sehen uns in der Pflicht, Maßnahmen zur Informationssicherheit in unternehmenskritischen Geschäftsprozessen zu implementieren und im Rahmen eines Informationssicherheitsmanagementsystems aufrecht zu erhalten.

3. Geltungsbereich

Diese Richtline gilt für die Inworks GmbH und betrifft alle Kunden, Partner und Beschäftigte der Inworks GmbH.

4. Informationssicherheitsziele

Bei der Planung und Ausübung unserer Geschäftsprozesse werden wir technische und organisatorische Maßnahmen zur Verfügbarkeit, Integrität und Vertraulichkeit und darüber hinaus zur Transparenz und Revisionsfähigkeit unserer Daten und Informationen einbeziehen und deren Umsetzung sicherstellen.

Den gesetzlichen und vertraglichen Anforderungen an die Informationssicherheit ist in besonderem Maße nachzukommen, so dass das Risiko von Sicherheitsvorfällen und Schadenseinflüssen gemindert werden kann.

4.1 Ziele und Risiken

Die sichere Softwareentwicklung und Erbringung der dazugehörigen Dienstleistungen (Customizing, Consulting, Support und Hosting) hängen maßgeblich von den verbundenen Prozessen ab. Die Ziele unseres ISMS sind

- die Einhaltung von gesetzlichen Vorgaben (Compliance)
- der Schutz von Betriebsgeheimnissen und vertraulichen Informationen
- die sichere Entwicklung und Bereitstellung unserer Lösungen (SaaS)
- die sichere Abwicklung von Dienstleistungen und Projekten für unsere Kunden

Vor diesem Hintergrund ist die Sicherstellung der Informationssicherheit davon abhängig, dass bestehende Risiken für die genannten Ziele erkannt werden, durch geeignete Maßnahmen vermieden bzw. gemindert und verbleibende Risiken geeignet behandelt bzw. Restrisiken durch die Geschäftsführung betrachtet und ggf. akzeptiert werden. Die geschieht im Inworks Risikomanagementsystem.

4.2 Bedeutung der Sicherheit

Vor dem Hintergrund der Sicherheitsanforderungen der Softwareentwicklung und der dazugehörigen Dienstleistungen (Customizing, Consulting, Support und Hosting) im Bereich Feedback- und Qualitätsmanagement muss Informationssicherheit ein integraler Bestandteil der Unternehmenskultur sein.

Jeder Mitarbeiter/jede Mitarbeiterin im Rahmen des Anwendungsbereichs muss sich der Notwendigkeit der Informationssicherheit bewusst sein und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg kennen.

5. Verpflichtung und Verantwortung

Wir als Geschäftsführung der Inworks GmbH verabschieden diese Leitlinie zur Informationssicherheit als Bestandteil der organisationsweiten Sicherheitsstrategie. Wir verpflichten uns dazu

- die Informationssicherheit als ein integraler Bestandteil der Informationssysteme über ihren gesamten Lebenszyklus zu sehen
- das Informationssicherheitsmanagementsystem durch organisatorische und technische Maßnahmen zu pflegen und kontinuierlich zu verbessern
- die Sicherheitsorganisation und den Sicherheitsprozess aktiv zu unterstützen

Das Unternehmen wird sich an dem Standard ISO/IEC 27001 orientieren und die Management-Elemente dieses Standards realisieren. Diese umfassen die Durchführung von regelmäßigen internen Audits, eine geeignete Steuerung der Dokumentation und der Aufzeichnungen, eine Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung (PDCA).

Jeder Mitarbeiter/jede Mitarbeiterin ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.

6. Sicherheitsorganisation

Der Sicherheitsorganisation werden von der Geschäftsführung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren.

Die Sicherheitsorganisation ist frühzeitig in alle zu berücksichtigenden Projekte einzubinden, um bereits in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten (DSB).

Zentrale Aufgaben der Sicherheitsorganisation sind

- Hinwirken auf die Einhaltung und Verbesserung sämtlicher Maßnahmen zur Informationssicherheit
- Erarbeiten von Konzepten und Lösungsvorschlägen für kritische Geschäftsprozesse und Verfahren innerhalb des Geltungsbereiches
- Kontrolle und Überprüfung der getroffenen Maßnahmen zur Informationssicherheit hinsichtlich Wirksamkeit und Angemessenheit

(Zuständige Personen sind im Organisationshandbuch in der Inworks definiert)

Informationssicherheitsbeauftragter (ISB)

Wir als Geschäftsführung benennen einen Informationssicherheitsbeauftragten (ISB), welcher, unterstützt durch eine Sicherheitsorganisation, den Informationssicherheitsprozess initiiert, plant, umsetzt, aufrechterhält und verbessert. Der ISB ist berechtigt, bei Gefahr im Verzug in Form von Angriffen auf das Unternehmen oder zur Abwendung von erheblichen Schäden in Abstimmung mit der Geschäftsführung geeignete Abwehrmaßnahmen zu ergreifen. Dies bedeutet z.B. IT-Prozesse oder IT-Systeme ggf. zu isolieren oder stillzulegen sowie andere geeignete Abwehrmaßnahmen zu ergreifen.

Datenschutzbeauftragter (DSB)

Wir bestellen wir einen Datenschutzbeauftragten (DSB). Er ist bei der Ausübung seiner Funktion weisungsfrei und berät Geschäftsführung, Personalvertretung und Mitarbeiter zu Datenschutzfragestellungen und adressiert die zur Umsetzung notwendigen Maßnahmen. Der DSB hat in Abstimmung mit der Geschäftsführung das jederzeitige Zutrittsrecht zu allen Stellen des Unternehmens in dem für seinen Aufgabenbereich erforderlichen Umfang.

Informationssicherheits- und Datenschutzkoordinator (ISK und DSK)

Der Informationssicherheitskoordinator ist in Abstimmung mit dem ISB die Umsetzung und Verbesserung der Informationssicherheit bei Inworks verantwortlich. Er vertritt den ISB im Unternehmen (in Abstimmung mit dem ISB oder der GF). Er berichtet direkt an den ISB und die Geschäftsleitung. Gleiches gilt entsprechend für den Datenschutzkoordinator.

Informationssicherheits- und Datenschutzkoordinatoren sind ermächtigt Audits durchzuführen, die Aufschluss über die tatsächliche Einhaltung der Schutzziele geben. Sie haben in Abstimmung mit der Geschäftsführung das jederzeitige Zutrittsrecht zu allen Stellen des Unternehmens in dem für die Aufgabenbereiche erforderlichen Umfang.

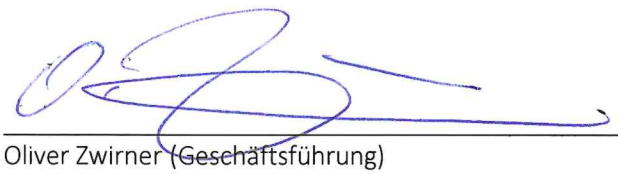
7. Sicherheitsmaßnahmen

Maßnahmen werden insbesondere in den Bereichen Technik und Organisation, Personal, Infrastruktur und Recht zu erarbeitet und umgesetzt.

Sämtliche Maßnahmen werden dabei in einem angemessenen wirtschaftlichen Verhältnis zum jeweils angestrebten Schutzbedarf der Daten und Informationen stehen und in Bezug auf die dynamische Entwicklung des Unternehmens sorgfältig ausgewählt.

Diese Leitlinie ist gültig ab dem 16.07.2024 und wurde von der Geschäftsführung freigegeben. Aktualisierte Versionen ersetzen die jeweils vorherigen Versionen.

Ulm, den 06.02.2025



Oliver Zwirner (Geschäftsführung)