Informationssicherheitspolitik

Inseya AG – Wir leben, was wir empfehlen.

Zweck und Geltungsbereich

Die Inseya AG bezweckt die ganzheitliche Bedienung ihrer Kunden im IT-Bereich und insbesondere im Bereich Cybersecurity. Dies umfasst strategische und operationelle Beratung, Planung, Realisierung und Betrieb aller nötigen Komponenten technischer und organisatorischer Natur, Outsourcingdienstleistungen, Service Providing sowie den Handel mit Soft- und Hardware.

Diese Informationssicherheitspolitik beschreibt die grundlegende Ausrichtung der Inseya AG zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Als Cybersecurity-Unternehmen sind wir uns bewusst, dass unsere eigene Informationssicherheit die Grundlage des Vertrauens ist, das unsere Kunden in uns setzen. Diese Politik gilt daher gleichermassen nach innen wie nach aussen: Sie ist unser tägliches Versprechen an unsere Kunden, Partner und Mitarbeitenden.

Diese Informationssicherheitspolitik gilt für alle Mitarbeitenden, externen Mitarbeitenden, Dienstleister und Partner, die im Geltungsbereich des ISMS tätig sind oder Zugriff auf Informationen und Systeme der Inseya AG haben. Die Inseya AG orientiert sich dabei an den Anforderungen der ISO/IEC 27001:2022.

Grundsätze der Informationssicherheit

Die Inseya AG schützt Informationen angemessen vor unbefugtem Zugriff, Verlust, Veränderung, Missbrauch, Offenlegung, Störung und Ausfall. Informationssicherheit wird risikobasiert, angemessen und nachvollziehbar umgesetzt. Dabei gelten insbesondere folgende Grundsätze:

- Informationen werden entsprechend ihrem Schutzbedarf klassifiziert und behandelt.
- Das Prinzip der minimalen Rechtevergabe gilt ausnahmslos: Zugriff auf Informationen und Systeme erhalten nur berechtigte Personen.
- IT-Systeme und Dienste werden angemessen gegen Störungen, Angriffe und Ausfälle geschützt.
- Gesetzliche, regulatorische, vertragliche und normative Anforderungen werden berücksichtigt, insbesondere das revidierte Schweizer Datenschutzgesetz (nDSG) und die ISO/IEC 27001:2022.
- Informationssicherheitsrisiken werden regelmässig identifiziert, bewertet und behandelt.
- Sicherheitsvorfälle werden unverzüglich gemeldet, strukturiert analysiert und mit klar definierten Massnahmen bearbeitet. Die Erkenntnisse fliessen systematisch in die Verbesserung des ISMS ein.
- Mitarbeitende werden regelmässig sensibilisiert und tragen aktiv zur Informationssicherheit bei.
- Das ISMS wird regelmässig überprüft, gemessen und kontinuierlich verbessert.

Verantwortung

Die Geschäftsführung der Inseya AG trägt die Gesamtverantwortung für das ISMS und stellt angemessene Rahmenbedingungen, Rollen, Verantwortlichkeiten und Ressourcen bereit.
Alle Personen, die im Geltungsbereich des ISMS tätig sind oder Zugriff auf Informationen und Systeme der Inseya AG haben, sind verpflichtet, die Vorgaben zur Informationssicherheit einzuhalten und Sicherheitsereignisse unverzüglich zu melden.

Kontinuierliche Verbesserung

Die Inseya AG überprüft die Wirksamkeit ihrer Informationssicherheitsmassnahmen regelmässig. Auf Basis von Risiken, Auditergebnissen, Sicherheitsvorfällen, regulatorischen Entwicklungen und Managementbewertungen wird das Informationssicherheitsniveau fortlaufend weiterentwickelt.

Informationssicherheit ist für uns kein Projekt mit Enddatum, sondern eine dauerhaft gelebte Unternehmenskultur. Wir verstehen sie als Qualitätsmerkmal und als messbaren Beitrag zum Vertrauen unserer Kunden und zur Resilienz unseres Unternehmens.

Genehmigt durch die Geschäftsleitung der Inseya AG