Informationssicherheit-Leitlinie

Information Security Policy

Veröffentlicht am 16.12.2024

Öffentlich

Hinweis: Im Interesse der Lesefreundlichkeit wird im Text meist nur eine Geschlechtsform verwendet. Selbstverständlich sind stets alle Geschlechter gleichermaßen angesprochen.

Inhaltsverzeichnis

1. Inkrafttreten

Diese Informationssicherheitsrichtlinie tritt zum 16.12.2024 in Kraft und wird allen Mitarbeiterinnen und Mitarbeitern sowie unseren Kunden und Auftragnehmern kenntlich gemacht. Darüber hinaus wird diese Informationssicherheitsrichtlinie in webseitentauglicher Form auch auf unserer Homepage isacon.com veröffentlicht.

Weinheim, 16.12.2024	Unterschriften der Geschäftsführung
Achim Baumgärtner	Sascha Jozic

2. Verpflichtung der Geschäftsführung

Wir, die Geschäftsführung der isacon AG, erkennen die essenzielle Bedeutung der Informationssicherheit in unserem Unternehmen uneingeschränkt an. In einer zunehmend digitalisierten Welt, die von wachsenden Informationssicherheits-Bedrohungen und strengen Datenschutzanforderungen geprägt ist, übernehmen wir die volle Verantwortung für den Schutz sensibler Daten und die Wahrung der Integrität unserer Systeme. Der Schutz aller Informationen, unabhängig von ihrer Form oder ihrem Medium, ist für uns eine unbedingte Grundlage, um das Vertrauen unserer Kunden, Partner und Mitarbeiter zu sichern.

Wir verpflichten uns, ein Informationssicherheitsmanagementsystem (ISMS) zu etablieren, das nicht nur gesetzliche Anforderungen erfüllt, sondern auch proaktiv Risiken identifiziert, bewertet und minimiert. Dieses Managementsystem bildet die Basis für die kontinuierliche Verbesserung unserer Sicherheitsmaßnahmen und stellt sicher, dass wir auf Sicherheitsvorfälle schnell und effektiv reagieren können.

Wir fördern eine Sicherheitskultur, in der sich jeder Mitarbeiter seiner Verantwortung bewusst ist

und aktiv zur Sicherheit unserer Informationen beiträgt. Wir verpflichten uns zu den höchsten Standards in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit unserer Daten und Systeme und werden dafür fortlaufend die notwendigen Mittel bereitstellen und auch selbst aktiv mitarbeiten.

Mit der Einführung eines ISMS und dessen konsequenter Integration in die Prozesse der Organisation stärken wir das Vertrauen unserer Kunden, Partner und Mitarbeiter und sichern die langfristige Resilienz unseres Unternehmens gegenüber den Herausforderungen der analogen und digitalen Welt. Wir, die Geschäftsführung, übernehmen die volle Verantwortung für die Umsetzung dieser Sicherheitsstrategie und garantieren, dass unsere Ziele der Informationssicherheit ohne Kompromisse erreicht werden.

3. Geltungsbereich

Diese Informationssicherheitsleitlinie erstreckt sich auf alle Tätigkeitsbereiche der isacon AG. Sie ist von sämtlichen Mitarbeitern zu beachten und strikt einzuhalten. Externe Dienstleister sind im Rahmen ihrer Beauftragung über die Leitlinie zu informieren und zur Einhaltung verbindlich zu verpflichten. Zudem stellt die isacon AG sicher, dass diese Leitlinie auch ihren Kunden aktiv kommuniziert wird, um Transparenz zu gewährleisten und gemeinsame Standards in der Informationssicherheit zu fördern.

4. Stellenwert der Informationssicherheit

Informationssicherheit ist für Unternehmen von zentraler Bedeutung, da sie nicht nur den Schutz sensibler Daten und Systeme sicherstellt, sondern auch Vertrauen schafft, Wettbewerbsfähigkeit stärkt und unternehmerische Werte langfristig bewahrt.

Die isacon AG verfolgt das Ziel, die Verfügbarkeit von Informationen in allen Bereichen so abzusichern, dass nur minimale Stillstandzeiten und tolerierbarer Informationsverluste entstehen können. Gleichzeitig wird großer Wert auf den umfassenden Schutz der Integrität und Vertraulichkeit aller Informationen gelegt, um finanzielle Schäden und Imageschäden konsequent zu vermeiden.

Einschränkungen bei der Verfügbarkeit unternehmenseigener Applikationen oder Verstöße gegen die

Integrität und Vertraulichkeit von Informationen können gravierende Folgen haben. Dabei gehen Bedrohungen nicht nur von externen Angriffen aus, sondern können auch durch interne Schwachstellen entstehen.

Ein hoher Standard der Informationssicherheit bietet der isacon AG zudem einen klaren Wettbewerbsvorteil, auch bei Ausschreibungen und der Gewinnung qualifizierter Mitarbeiter.

5. Zweck dieser Leitlinie

Die IT-Sicherheitsleitlinie der isacon AG verfolgt das Ziel, alle berechtigt interessierten Parteien für die Bedeutung der Informationssicherheit zu sensibilisieren, die Maßnahmen der isacon AG zu kommunizieren und nachhaltige Verbesserungsmaßnahmen anzustoßen. Sie bietet einen Überblick über die Unternehmensziele sowie die damit verbundenen Informationssicherheitsziele.
Darüber hinaus definiert die Leitlinie die Verantwortlichkeiten im Bereich der Informationssicherheit und beschreibt die Rolle der jeweiligen Akteure bei der Sicherung und Weiterentwicklung von Sicherheitsmaßnahmen. Sie bildet zudem die Grundlage für die schrittweise Einführung eines Informationssicherheitsmanagementsystems und markiert damit einen wesentlichen Meilenstein im kontinuierlichen Sicherheitsprozess der isacon AG.

6. Unsere Grundsätze der Informationssicherheit

Die folgenden Grundsätze bilden die Grundlage der Informationssicherheit der isacon AG und sind zwingend zu beachten und einzuhalten.

Minimalprinzip des Zugriffs

Jeder Mitarbeiter erhält nur so viel Zugriff auf Systeme und sensible Informationen, wie zur Erfüllung der jeweiligen Aufgaben unbedingt erforderlich ist. Diese Vorgehensweise schützt vor unautorisierten Zugriffen und sichert die IT-Systeme.

Maximalprinzip des Schutzes

Je nach Schutzbedarf sind unterschiedliche Maßnahmen erforderlich, um einen reibungslosen und sicheren Betrieb zu gewährleisten. Daher ist für jede Nutzung eine geeignete Schutzstrategie festzulegen.

Sensibilisierung der Mitarbeiter

Von allen Mitarbeitern wird ein verantwortungsbewusster Umgang mit schützenswerten Informationen und Systemen erwartet. Das gesamte Personal muss den Informationssicherheits-prozess aktiv unterstützen. Führungskräfte sollten sich ihrer Vorbildfunktion bewusst sein und diese aktiv leben.

Dokumentation und Weiterentwicklung

Alle Sicherheitsmaßnahmen sind sorgfältig zu dokumentieren und regelmäßig anzupassen, um ein konstantes Schutzniveau sicherzustellen. Alle Sicherheitsvorfälle sind zu dokumentieren und zu analysieren, um getroffene Maßnahmen bewerten zu können. Eine jährliche Überprüfung der Maßnahmen soll dabei gewährleistet sein.

7. Unsere Sicherheitsziele

Bewusstsein für Informationssicherheit bei allen Mitarbeitern

Die Gewährleistung der Informationssicherheit erfordert sowohl organisatorische, persönliche, physische als auch technische Maßnahmen. Diese sind nur dann effektiv, wenn alle Mitarbeiter die potenziellen Gefährdungen kennen und entsprechend verantwortungsbewusst handeln.

Einhaltung von Gesetzen und Vorschriften

Die Maßnahmen zur Informationssicherheit sollen zudem sicherstellen, dass alle relevanten gesetzlichen Vorgaben, vertraglichen Verpflichtungen und Unternehmensvorschriften eingehalten werden.

Verfügbarkeit der Informationen

Relevante Informationen müssen für berechtigte Mitarbeiter jederzeit verfügbar sein. Sie müssen im Notfall schnell wiederhergestellt werden können. Systemausfälle sind zu vermeiden, um die Geschäftskontinuität zu gewährleisten.

Vermeidung materieller Schäden

Veränderungen an Daten, der Verlust der Vertraulichkeit schutzbedürftiger Informationen oder der Ausfall von IT-Systemen können sowohl materielle als auch finanzielle Schäden verursachen, die es zu verhindern gilt.

Wahrung von Persönlichkeitsrechten und Betriebsgeheimnissen

Die Vertraulichkeit und Integrität aller für das Unternehmen wichtigen Informationen müssen geschützt werden, unabhängig von ihrer Form. Im Umgang mit elektronischen Daten und Dokumenten und auch in der mündlichen Kommunikation sind die Geheimhaltungsanweisungen strikt zu befolgen, um Persönlichkeitsrechte und Betriebsgeheimnisse zu wahren.

8. Sicherheitsstrategie und Aufbauorganisation

Diese Informationssicherheitslinie beschreibt das Informationssicherheitsmanagement der isacon AG, mit dem Ziel, ein angemessenes Sicherheitsniveau zu gewährleisten. Begleitend zu dieser Leitlinie stellt das ISMS themen-spezifische Richtlinien bereit.

Dazu wurde ein risikobasiertes Vorgehen gewählt. In regelmäßigen Abständen werden alle Risiken der Informationssicherheit bei der isacon erhoben, bewertet und priorisiert. Die Höhe des Risikos bestimmt dabei maßgeblich den Inhalt und Umfang der Maßnahme und auch die zeitliche Frist bis zum Inkrafttreten der Maßnahme.

Die Organisationsleitung hat eine Person ernannt, die als erster Ansprechpartner für alle Fragen zur Informationssicherheit fungiert. Er berichtet direkt an die Organisationsleitung und steht in regelmäßigem Austausch mit der IT-Leitung. Die Person bekommt die Rolle

Informationssicherheitsbeauftragte/r (ISB oder engl. ISO).

In regelmäßigen Abständen überprüft dieser, ob die bestehenden Sicherheitsmaßnahmen noch ausreichend sind. Wenn nicht, werden Gegenmaßnahmen eingeleitet. Im Falle eines Sicherheitsvorfalls informiert der Informationssicherheitsbeauftragte die Organisationsleitung oder den Verfahrensverantwortlichen und kooperiert bei Bedarf mit externen Organisationen und staatlichen Stellen.

- Maßnahmen, die die Informationssicherheit betreffen oder Änderungen im Informationssicherheits-Managementsystem (ISMS) bewirken, werden stets nach dem 4-Augen-Prinzip umgesetzt. Vor der Durchführung werden die Aufgaben sorgfältig geprüft, von einer zweiten Person genehmigt und dokumentiert. Eine nachfolgende Prüfung trägt Sorge dafür, dass keine unbefugten oder unbeabsichtigten Änderungen erfolgt sind. Zusätzlich wird auf eine klare Rollentrennung geachtet, um Interessenkonflikte zu vermeiden und die Integrität der Prozesse zu sichern.

Externe Personen und Unternehmen, die Leistungen für die isacon AG erbringen, sind vertraglich zur Einhaltung festgelegter Informationssicherheitsziele verpflichtet. Bei der Verarbeitung personenbezogener Daten sind zusätzlich die Regelungen der Datenschutzgrundverordnung zu beachten.

Die erforderlichen Personal- und Finanzmittel werden bereitgestellt, um ein angemessenes Informationssicherheitsniveau bei der Verarbeitung schützenswerter Daten zu gewährleisten. Für den Informationssicherheitsbeauftragten werden alle notwendigen Ressourcen und Qualifizierungsmaßnahmen zur Erfüllung seiner Aufgaben bereitgestellt. Zudem werden Mitarbeiter regelmäßig in IT-Sicherheit geschult und für die Belange der Informationssicherheit sensibilisiert.

Die Verantwortlichkeiten im Bereich der Informationssicherheit bei der isacon AG sind wie folgt strukturiert:

Organisationsleitung

Die Geschäftsführung trägt die Gesamtverantwortung für alle Aspekte der Informationssicherheit der isacon AG.

Informationssicherheitsbeauftragte

Die/Der Informationssicherheitsbeauftragte (ISB) ist verantwortlich für die regelmäßige Information der Organisationsleitung über den Stand der Informationssicherheitsmaßnahmen und deren Umsetzung. Er organisiert Schulungen zur Sensibilisierung des Personals und fördert das Bewusstsein für Informationssicherheit.
Bei der Beschaffung neuer Systeme und der Implementierung neuer Verfahren ist der ISB frühzeitig einzubinden. Die Freigabe erfolgt in Abstimmung mit der Organisationsleitung. In Bezug auf die Erfüllung seiner Aufgaben ist der ISB ausschließlich an Weisungen der Organisationsleitung gebunden.

Er steht als Berater bei Fragen zur Informationssicherheit zur Verfügung und untersucht sowie meldet sicherheitsrelevante Ereignisse an die zuständigen Stellen. Die kontinuierliche Weiterentwicklung des ISMS wird maßgeblich vom ISB gesteuert. Der ISB übernimmt nicht die technische Umsetzung.

Technischer IT Security Lead

Der Technische IT Security Lead ist verantwortlich für die technische Umsetzung und Leitung aller IT-Sicherheitsmaßnahmen. Er entwickelt IT-Sicherheitsstrategien, setzt Lösungen um, koordiniert IT-Teams und leitet das Incident-Management-Team. Zudem arbeitet er eng mit dem Informationssicherheitsbeauftragten zusammen, ist zentraler Ansprechpartner für technische Sicherheitsfragen und sorgt für die Abwehr komplexer Bedrohungen sowie die Einhaltung von Compliance-Anforderungen.

Datenschutzbeauftrage

Der Datenschutzbeauftragte (DSB) wird extern bestellt, um objektive und unvoreingenommene

Beratung zu gewährleisten, Interessenkonflikte zu vermeiden und die unabhängige sowie effektive Umsetzung der Datenschutzvorgaben sicherzustellen.

Mitarbeitende

Alle Mitarbeitenden müssen sich ihrer Verantwortung im Umgang mit den Systemen und den darauf verarbeiteten Informationen stets bewusst sein. Im Falle von Auffälligkeiten oder Unregelmäßigkeiten im Betrieb ist der Informationssicherheitsbeauftragte unverzüglich zu informieren, um frühzeitig Gegenmaßnahmen ergreifen und Ausfälle verhindern zu können.

Mitarbeiter sind verpflichtet, an den Awareness-Schulungen teilzunehmen und die Maßnahmen zur Informationssicherheit aktiv zu unterstützen. Bei Bedarf unterstützen Mitarbeiter den ISB oder den technischen IT-Sec-Lead.

9. Kontinuierliche Weiterentwicklung

Der isacon AG verpflichtet sich zur kontinuierlichen Weiterentwicklung der Informationssicherheit. Das heißt, der Status Quo ist für uns nicht gut genug, wir wollen immer besser werden.

Informationssicherheit-Leitlinie

Final Audit Report 2024-12-17

Created:	2024-12-16
By:	Sascha Jozic (sj@isacon.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAS4OY8XFg4I2JH0cbbe70CAS_frinYD6n

"Informationssicherheit-Leitlinie" History

Document created by Sascha Jozic (sj@isacon.com)
2024-12-16 - 3:00:46 PM GMT- IP address: 188.74.0.123

Document emailed to Achim Baumgärtner (achim.baumgaertner@isacon.com) for signature
2024-12-16 - 3:00:52 PM GMT

Email viewed by Achim Baumgärtner (achim.baumgaertner@isacon.com)
2024-12-17 - 11:55:17 AM GMT- IP address: 82.83.152.20

Document e-signed by Achim Baumgärtner (achim.baumgaertner@isacon.com)
Signature Date: 2024-12-17 - 11:57:46 AM GMT - Time Source: server- IP address: 82.83.152.20

Agreement completed.
2024-12-17 - 11:57:46 AM GMT