



# ISO 27001: Informationssicherheits- managementsystem

# Inhalt

---

<b>Einleitung</b>	<b>3</b>
<b>Geltungsbereich</b>	<b>4</b>
<b>Richtlinien und Erklärungen</b>	<b>5</b>
<b>Asset-Management</b>	<b>7</b>
<b>Systematischen Ansatz</b>	<b>8</b>
<b>Physische Sicherheit</b>	<b>9</b>
<b>Betriebssicherheit</b>	<b>11</b>
<b>Kommunikationssicherheit</b>	<b>13</b>
<b>Störungsmanagement</b>	<b>14</b>
<b>Geschäftskontinuität</b>	<b>14</b>
<b>Compliance</b>	<b>15</b>

---

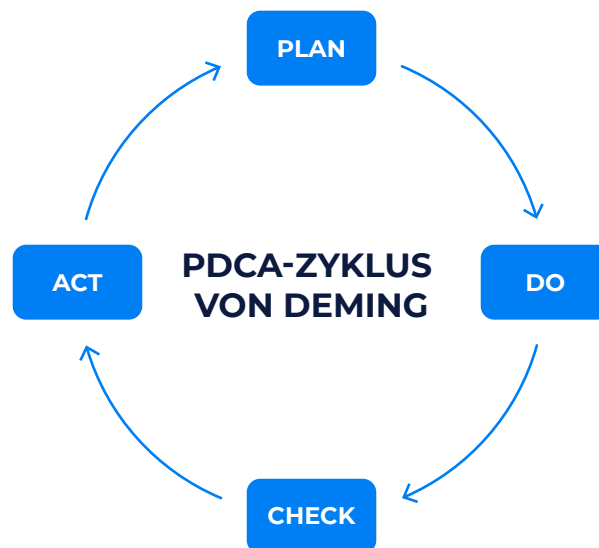
# Einleitung

SaM Solutions ist ein internationaler Softwareentwicklungsdienstleister mit mehr als 25 Jahren Erfahrung auf dem Markt der Informationstechnologie. Die Haupttätigkeitsbereiche des Unternehmens sind die kundenspezifische Softwareentwicklung auf den amerikanischen und europäischen Märkten sowie Beratungsleistungen in den Entwicklungsprozessen. Fragen der Informationssicherheit und des Datenschutzes zählen zu den Hauptprioritäten des Unternehmens und rechtfertigen das hohe Vertrauen unserer Kunden, unter denen sich weltweit führende Unternehmen verschiedener Branchen befinden. Um die Einhaltung der gesetzlichen Anforderungen der Europäischen Union sowie die Kundenanforderungen im Bereich der Informationssicherheit zu bestätigen, hat die Unternehmensleitung beschlossen, **ein Informationssicherheitsmanagementsystem gemäß ISO 27001 zu implementieren**. SaM Solutions hat erfolgreich die Systemzertifizierung durch eine renommierte internationale Zertifizierungsstelle erhalten.

Der Zweck dieser Übersicht besteht darin, alle interessierten Parteien über die allgemeinen Aspekte der Informationssicherheit und des Schutzes personenbezogener Daten durch SaM Solutions zu informieren. Alle diese Anforderungen und Maßnahmen sind als Standards, Richtlinien und Leitlinien des Unternehmens dokumentiert und an alle Mitarbeiter kommuniziert worden. Aus Sicherheitsgründen beschreibt dieses Dokument nicht die spezifischen Verfahren, Tätigkeiten und Methoden, die durchzuführen sind.

# Geltungsbereich

Das **Informationssicherheitsmanagementsystem** von SaM Solutions ist auf dem Modell des **PDCA-Zyklus von Deming (Plan–Do–Check–Act)** aufgebaut, der die Anforderungen der ISO-Normen vollständig erfüllt und die Entwicklung und den effektiven Betrieb des Systems ermöglicht.



Der Geltungsbereich des Systems umfasst weltweite Entwicklungszentren und den Hauptsitz in Deutschland, wodurch es möglich ist, die hohen Anforderungen an den Informationsschutz in allen Phasen der Softwareentwicklung zu erfüllen:

- ***DE: Konzeption, Design, Entwicklung und Wartung von Softwarelösungen. Projektmanagement und Implementierung***

Der Geltungsbereich der Zertifizierung umfasst alle Prozesse des Unternehmens in allen Betriebsphasen, insbesondere den Projektmanagementprozess, der auch das Vertrag- und Liefermanagement miteinschließt.

# Richtlinien und Erklärungen

Um die strategischen Aspekte der Aktivitäten und die Einstellung zu Sicherheitsfragen zu definieren, wurden entsprechende Informationssicherheitsrichtlinien entwickelt und öffentliche Erklärungen abgegeben. Alle Dokumente sind auf der offiziellen Webseite von SaM Solutions öffentlich zugänglich.

## Die Richtlinie für das Informationssicherheitsmanagementsystem erklärt Folgendes:

Das Hauptziel, das mit allen Bestimmungen dieser Richtlinie erreicht werden soll, ist der Schutz von Informationsressourcen und Daten, einschließlich personenbezogener Daten von Einzelpersonen, vor jeglichen Schäden, die durch versehentliche oder absichtliche Eingriffe in das Informationssystem des Unternehmens oder im Falle von Informationssicherheitsvorfällen verursacht werden.

Bei der Durchführung ihrer Aktivitäten im Bereich der Zertifizierung "**Konzeption, Design, Entwicklung und Wartung von Softwarelösungen. Projektmanagement und Implementierung**", übernimmt SaM Solutions die folgenden Verpflichtungen:

- Einhaltung der nationalen Gesetzgebung und der geltenden internationalen Gesetze, Normen und Vorschriften im Bereich der Informationssicherheit.
- Verhinderung der unbefugten oder unsachgemäßen Nutzung von Informationsressourcen und Informationssystemen.
- Zertifizierte Antivirensoftware zu verwenden und Malware-Infektionen zu vermeiden sowie alle Vorfälle im Bereich der Informationssicherheit zu untersuchen.
- Ausschließlich lizenzierte Software in den Informationssystemen des Unternehmens zu verwenden.
- Informationen zu klassifizieren, Assets zu identifizieren und zu bewerten, Bedrohungen und Schwachstellen zu erkennen, Risiken zu managen und Objekte der Informatisierung

zu klassifizieren, um die Sicherheit und Fehlertoleranz von Informationssystemen zu gewährleisten.

- Wirksame Maßnahmen zu ergreifen, um die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen und Daten sowie die Aktualität von Hard- und Software zu gewährleisten, um das erforderliche Niveau der Sicherheit des Informationssystems aufrechtzuerhalten.
- Sicherstellung des unterbrechungsfreien Betriebs des Informationssystems, seiner Fehlertoleranz und der schnellen Wiederherstellung im Falle von Informationssicherheitsvorfällen.
- Die kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems und die Einhaltung der Zertifizierungsanforderungen zu gewährleisten.
- Die Richtlinie des Informationssicherheitsmanagementsystems auf dem neuesten Stand zu halten und sie an Geschäftspartner, Dritte und Mitarbeiter zu kommunizieren.

Um die oben genannten Verpflichtungen zu erfüllen und das reibungslose Funktionieren des Informationssicherheitsmanagementsystems zu gewährleisten, garantiert die Geschäftsleitung von SaM Solutions die Bereitstellung aller notwendigen Ressourcen.

Neben der **Richtlinie zum Informationssicherheitsmanagementsystem** hat SaM Solutions eine Reihe weiterer Richtlinien angenommen und Erklärungen im Bereich des Schutzes von Informationen und personenbezogenen Daten abgegeben:

- 1. Richtlinie zum Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten — beschreibt die Ziele, die sich SaM Solutions für den Schutz personenbezogener Daten von natürlichen Personen gesetzt hat, sowie die Art und Weise, wie diese Ziele erreicht werden.
- 2. Erklärung zur Verarbeitung personenbezogener Daten** — beschreibt die Zwecke, Art und Methoden der Erhebung und Verarbeitung personenbezogener Daten von natürlichen Personen durch das Unternehmen.
- 3. Richtlinie zur Informationssicherheit Dritter** — beschreibt die Beziehungen und Anforderungen, die SaM Solutions an Lieferanten und Subunternehmer stellt.

Detaillierte Richtlinien finden Sie auf der Webseite von SaM Solutions. Die ausgegebenen Dokumente ermöglichen eine transparente Beschreibung der Grenzen der Interaktion und des verantwortungsvollen Umgangs des Unternehmens mit Sicherheitsfragen.

# Asset-Management

Das **Asset-Management** ist einer der wichtigsten Aspekte eines systematischen Ansatzes für das Sicherheitsmanagement. SaM Solutions führt regelmäßig eine Inventarisierung, Buchhaltung und Bewertung der Assets durch. Allgemeine Managemententscheidungen zur Überarbeitung der Asset-Kategorien werden mindestens einmal pro Jahr getroffen. Die Assets werden unter Berücksichtigung aller Anforderungen der ISO-Normenreihe verwaltet. Mitarbeiter, die mit vertraulichen Informationen umgehen, sind unter anderem persönlich dafür verantwortlich, deren Sicherheit zu gewährleisten. Die entwickelten Kategorisierungssysteme und die verwendeten Methoden basieren nicht nur auf dem Wert der Assets, sondern berücksichtigen auch die Sicherheitsaspekte der Assets in Bezug auf ihre hierarchische Ebene.



## GESCHÄFTSEBENE

- Beziehung zwischen Assets und ihren Eigentümern
- Auswirkungen auf die geschäftlichen Aspekte des Unternehmens



## ANWENDUNGSEBENE

- Abhängigkeit der Assets von ihrem Zweck und ihrer Verwendung
- Gruppierung der Assets nach Anwendbarkeit und Zugriffskategorien



## PHYSIKALISCHE EBENE

- Beziehung zwischen Assets und ihrem Standort
- Berücksichtigung von Lokalisierungsaspekten von Assets

# Systematischen Ansatz

Der Entscheidungsprozess des Systemmanagements von SaM Solutions im Bereich der Informationssicherheit basiert auf **einem risikoorientierten Ansatz**. Das Unternehmen setzt in allen Phasen moderne Methoden und Modelle des Risikomanagements ein und führt jedes von ihnen auf eine strukturierte Weise durch:



- Risikoidentifikation und -bewertung der Wahrscheinlichkeit seiner Verwirklichung und des Ausmaßes der Folgen sowie die Bestimmung des maximal möglichen Schadens.
- Auswahl von Methoden und Werkzeugen, um das identifizierte Risiko zu bewältigen.
- Entwicklung einer Risikostrategie, um die Wahrscheinlichkeit der Risikoverwirklichung zu reduzieren und die möglichen negativen Folgen zu minimieren.
- Umsetzung der Risikostrategie.
- Bewertung der erzielten Ergebnisse und Anpassung der Risikostrategie.

Das Informationssicherheitsmanagementsystem wird regelmäßig vom Management überprüft. Interne Audits helfen, die Einhaltung der festgelegten Anforderungen zu klären sowie akzeptierte Bewertungskriterien in systemischen Aspekten zu verifizieren. Die oberste Führungsebene des Unternehmens ist auch an externen Audits beteiligt, wodurch die Einbeziehung des Managements in allen Aspekten des Systemmanagements sichergestellt wird. Die Erfahrungen aus den internen und externen Audits bilden die Grundlage für das kontinuierliche Verbesserungsmodell und bilden die Informationssicherheitsziele für den nächsten Berichtszeitraum.

# Physische Sicherheit

Die von der ISO 27001 geforderte physische Sicherheit ist unter Berücksichtigung der aktuellen technischen Anforderungen gewährleistet. Für einzelne Projekte und Kunden veranlasst SaM Solutions jedoch zusätzliche Schutzmaßnahmen auf der Grundlage von Vertragsbedingungen, die Anforderungen an Schutzbereiche enthalten können, welche über jene, die routinemäßig implementiert und verwendet werden, hinausgehen. Die Teams des Unternehmens sind erfahren in der Durchführung von Projekten mit streng vertraulichen Informationen in Umgebungen mit hohem Risiko und hohem Schutzbedarf.

Die folgenden dokumentierten physischen Sicherheitsvorkehrungen werden in Übereinstimmung mit ISO 27001 implementiert und verwendet:

## Zutritts- und Zugangskontrolle

---

Das Unternehmen bietet ein hohes Maß an Zugangskontrolle und protokolliert den Zutritt von Personen zu seinem Bereich und seinen Räumlichkeiten. Zu diesem Zweck wird ein Prozess der physischen Authentifizierung und Identifizierung sichergestellt, und die Zutrittsstufen werden in Kategorien unterteilt.

Alle Bereiche des Unternehmens sind mit einem Videoüberwachungssystem ausgestattet, das ein Videoarchiv und eine direkte Beobachtung der Kamerainformationen in Echtzeit nutzt.

Der Zugang zu den Bereichen erfolgt über elektronische Karten, die einen Authentifizierungsprozess unter Abgrenzung der Zugangsrechte sicherstellen.

Alle Büros werden mit physischen Schlüsseln verschlossen und die Schlüsselausgabe erfolgt zentral mit Protokollierung.

Die Bürotüren sind unter Berücksichtigung der Brandschutzanforderungen mit automatischen Schließvorrichtungen ausgestattet.

Verantwortliche, die mit vertraulichen Informationen umgehen, bewahren diese in verschlossenen Schränken und/oder Tresoren auf. Es wurden Richtlinien für den Umgang mit Informationen eingeführt, die die Verwendung gemeinsam genutzter Geräte (Netzwerkdrucker, Scanner, Faxgeräte, usw.) berücksichtigen.

## Abgangskontrolle

---

Die Kontrolle von Wechseldatenträgern richtet sich nach den jeweiligen Standards des Unternehmens und umfasst:

- das Führen von Aufzeichnungen über das Einführen/Entfernen von Geräten und anderen Vorrichtungen beim Betreten oder Verlassen von Gebäuden;
- die getrennte Aufbewahrung von vertraulichen Informationsträgern und, wenn möglich, deren besondere Kennzeichnung;
- die Verwendung von steckbaren Geräten einzuschränken, sofern angebracht.

## Sicherheitsbereiche

---

**Sicherheitsbereiche** sind Räume mit einem besonderen Zugangsmodus, die durch separate Zutrittskategorien abgegrenzt werden. Zu den Sicherheitsbereichen gehören Serverräume, Räume, die der Stromversorgung des Gebäudes dienen, und andere Räume, die auf der Grundlage einer Risikoanalyse klassifiziert wurden. Die physische Sicherheit von Sicherheitsbereichen wird durch geeignete Maßnahmen gewährleistet:

- Die Sicherheitsbereiche sind mit internen Videoüberwachungssystemen ausgestattet.
- Der Zugang zu den Sicherheitsbereichen ist nur mit einem Schlüssel und einer elektronischen Zugangskarte mit einer ordnungsgemäß programmierten Zugangskategorie möglich.
- Die Schlüssel werden an genau identifizierte Mitarbeiter des Unternehmens ausgegeben, die über die entsprechende Zutrittskategorie verfügen.

# Betriebssicherheit

Die Dokumentation des Informationssicherheitsmanagementsystems enthält etablierte **Betriebssicherheitsprozesse**, die sicherstellen, dass die folgenden Anforderungen vollständig umgesetzt werden:

- Es wird nur lizenzierte Software eingesetzt, alle Aktualisierungen, Patches und neuen Versionen werden rechtzeitig installiert.
- Zur Erkennung und Bekämpfung von Malware und bösartigem Code wird Antiviren-Software eingesetzt.
- Backup-Tools und -Systeme werden verwendet, um Informationen im Falle einer Verletzung ihrer Sicherheitseigenschaften wiederherzustellen.
- Ereignisse und Aktionen werden protokolliert und über ein automatisiertes System verbucht, um zu überwachen, ob die Hard- und Software zugänglich sind und ob irgendwelche Ausfälle in ihrer Funktionsweise vorliegen.
- Die periodische Überwachung von Protokollen und Ereignissen wird manuell auf Hardware, die auf der Grundlage der Risikoanalyse ausgewählt wurde, und für bestimmte Software durchgeführt.
- Software wird nur zentral von autorisiertem Personal installiert.
- An Geräten wird eine sicherheitstechnische Überprüfung durchgeführt, bevor sie nach dem Kauf, der Reparatur oder sonstigem Verlassen des Unternehmens in die Betriebsumgebung gebracht werden.

## Zugangskontrollen

---

Als Teil der Betriebssicherheitsaktivitäten werden spezielle Zugangskontrollmaßnahmen angewendet, um sicherzustellen, dass das Sicherheitsniveau der ISO 27001 entspricht. Zu den wichtigsten Anforderungen, die erfüllt werden müssen, gehören:

- Benutzerrechte und -rollen werden sowohl auf Intranet-Ebene als auch in den verschiedenen Anwendungen und Systemen des Unternehmens, wie z. B. Jira, Confluence, Azure und anderen, unterschieden;
- Benutzeraktionen für einzelne Systeme werden protokolliert und überwacht;

- Sicherheitseinstellungen in Active Directory, die für die notwendigen lokalen Geräteeinstellungen sorgen, wie z. B. das Sperren von Konten, wenn ein falsches Kennwort mehrmals eingegeben wird, das Sperren des Systems, wenn das Zeitlimit für die Benutzeraktivität abgelaufen ist, und andere;
- Führung und Sperrung von zentralisierten Abrechnungsunterlagen im Falle der Entlassung eines Mitarbeiters und/oder der Rückübertragung von Rechten im Falle der Versetzung eines Mitarbeiters in eine andere Abteilung oder in ein anderes Projekt.

Eine saubere Desktop-Richtlinie wurde eingeführt und angewendet.

## Systembeschaffung, -entwicklung und -wartung



**Der Software-Entwicklungslebenszyklus** (Software Development Life Cycle, SDLC) wird aufgebaut und dokumentiert, was es ermöglicht, Rollen und Verantwortlichkeiten in allen Phasen klar zu definieren und damit sowohl die Sicherheit der Projektumgebung als auch der zu verarbeitenden Informationen zu gewährleisten.

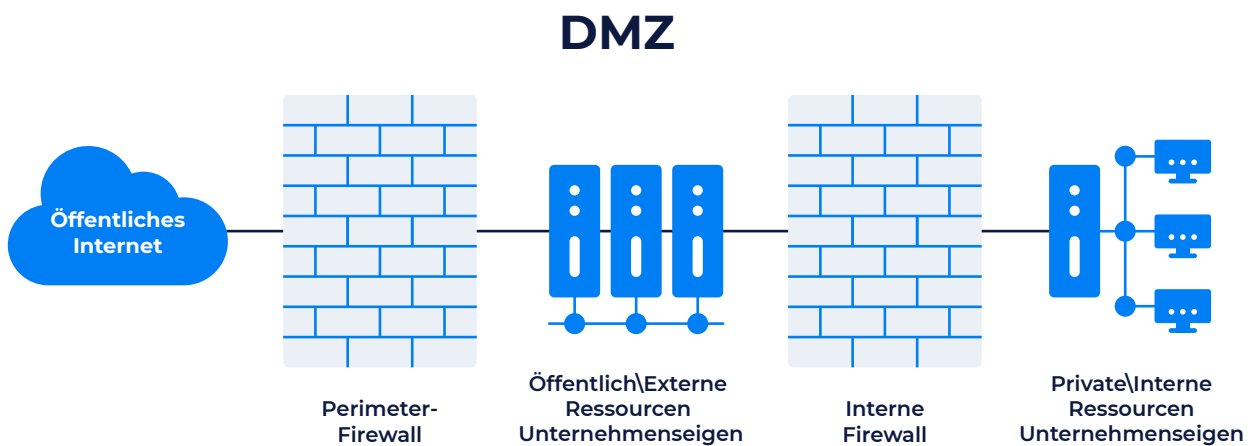
Alle wesentlichen Änderungen an der Projektumgebung und der Produktion werden von dazu autorisiertem Personal vorgenommen; entsprechend werden Änderungen an der Umgebung sowie an den Softwarepaketen zusätzlich kontrolliert.

Die Entwicklungssicherheit wird getestet, ebenso wie der Grad der Einhaltung von Sicherheitsstandards, und eine Reihe von Sicherheitsmustern und -werkzeugen werden vom Kunden festgelegt.

# Kommunikationssicherheit

Als Teil der **Kommunikationssicherheit** wird ein Diagramm von Netzwerken und Kommunikationen entwickelt und auf dem neuesten Stand gehalten. Die Trennung von Systemen und Netzwerken wird angewendet, einschließlich der Installation von Firewalls zwischen Segmenten.

Es wurde eine **Demilitarisierte Zone (DMZ)** geschaffen, in die Projekte und Projektsegmente mit direktem Zugang zum Internet verlagert werden. Die DMZ ist segmentiert und durch Firewalls von anderen Netzwerken getrennt, die Segmente der Produktionsumgebung sind von der Entwicklungs- und Testumgebung getrennt, welche nach Möglichkeit ebenfalls getrennt sind.



Für die Kommunikation zwischen Mitarbeitern und für die Interaktion mit Kunden wurden Beschränkungen auferlegt, was es ermöglicht, den Umgang mit vertraulichen Informationen zu kontrollieren. Innerhalb des Unternehmens werden bestimmte Messenger-Dienste für die Kommunikation genutzt, die zentral von autorisiertem Personal verwaltet werden.

Der Umfang der Kommunikation und die Eigenschaften werden durch einen speziellen Kodex definiert, der die Grundlagen der Unternehmenspolitik, den Kommunikationsstil und die Art und Menge der Informationen bei Verhandlungen oder Arbeitsaktivitäten umfasst.

# Störungsmanagement

SaM Solutions hat unter Berücksichtigung der Klassifizierung von Informationssicherheitsereignissen Verfahren für das **Störungsmanagement** dokumentiert. Es wurden Maßnahmen und Wege entwickelt, um auf Informationssicherheitsereignisse zu reagieren, die von der Überwachung über Untersuchungen bis hin zu Notfallmaßnahmen reichen. Alle Informationen über Informationssicherheitsvorfälle werden gespeichert und zur Verbesserung des Informationssicherheitsmanagementsystems im Allgemeinen und des Risikomanagements im Besonderen verwendet.

Als präventive Reaktion auf Informationssicherheitsereignisse werden regelmäßige Scans von Netzwerk- und Systemschwachstellen sowie Pentests durchgeführt.

# Geschäftskontinuität

Ein hohes Maß an Verantwortung gegenüber den Kunden ist eine der Prioritäten des Geschäftsbetriebs von SaM Solutions. Das Unternehmen hat eine Strategie der Widerstandsfähigkeit gegenüber verschiedenen Krisensituationen entwickelt, nach der die gesamte Infrastruktur des Unternehmens innerhalb von 24 Stunden nach ihrer vollständigen Zerstörung wiederhergestellt werden kann, z. B. im Falle von Naturkatastrophen oder militärischen Operationen.

Um die Fehlertoleranz und **Geschäftskontinuität** zu gewährleisten, werden moderne Technologien der Virtualisierung, Datensicherung und andere Best Practices im Bereich des Datenschutzes eingesetzt. Die Backups und Fehlertoleranz von Systemen und Netzwerken werden periodisch getestet.

# Compliance

Die Einhaltung der hohen Anforderungen an die Informationssicherheit wird durch regelmäßige Analysen und einen systematischen Ansatz in Bezug auf Sicherheit, Gegenmaßnahmen, die Entwicklung von Maßnahmen und Zielen zur Korrektur und Vorbeugung sowie die Überprüfung durch das Management sichergestellt. Der Nachweis der Compliance wird im Rahmen von internen Audits durchgeführt.

Jedes Jahr unterzieht sich SaM Solutions externen Audits durch eine internationale Zertifizierungsstelle, um die Einhaltung der ISO 27001 zu bestätigen. Auf diese Weise stellt das Unternehmen sicher, dass alle deklarierten Sicherheitsaspekte und übernommenen Compliance-Verpflichtungen von Dritten überwacht werden.

Ausgestellte Zertifikate mit dem aktuellen Zertifizierungsumfang sind auf der Webseite des Unternehmens [sam-solutions.com](https://www.sam-solutions.com) öffentlich zugänglich.



**SaM Solutions**

Tel.: +49-8105-77890

[www.sam-solutions.com](http://www.sam-solutions.com)

**Data Protection Officer:**

Alexandr Zorin

Chief Information Security Officer

E-mail: [dpo@sam-solutions.com](mailto:dpo@sam-solutions.com)