
# Leitlinie Informationssicherheit

| Informationen zum Dokument | |
|---|---|
| **Version** | 1.8 |
| **Dokument ID** | IS.LL02 |
| Klassifikation | Public |
| Status | Released |
| Ursprungsversion freigegeben durch | ISB, GF |
| Aktuelle Version freigeben durch | ISB |
| Review Zyklus | Jährlich |
| Gültig ab | 01.03.2018 |
| Dokumentendatum | 20.02.2024 |

# Inhaltsverzeichnis

# 1 Einleitung

**Glaube dich nicht allzu gut gebettet;**
**ein gewarnter Mann ist halb gerettet.**

***Johann Wolfgang von Goethe (1749 - 1832)***

*„Informationssicherheit ist uns bei siticom sehr wichtig und wird von allen Mitarbeitern gelebt, sowie in der täglichen Arbeit praktiziert."*

*„Unser Sicherheitsbewusstsein gepaart mit unserer Expertise qualifiziert siticom als einen verlässlichen und gewissenhaften Partner für unsere Kunden."*

*„Die uns anvertrauten Daten und Informationen werden stets zweckbestimmt behandelt und vor missbräuchlicher Verwendung geschützt."*

*„Informationssicherheit endet bei uns nicht bei unseren Mitarbeitern und Partnern, sondern umfasst alle geleisteten Dienstleistungen."*

Dieses Dokument ist die Leitlinie der siticom GmbH zur Informationssicherheit.

Das Ziel der Informationssicherheit ist die bestehende offene Unternehmenskultur mit einem State-of-the-Art Informationsschutz zu verbinden. Dies bedeutet, dass die Vertraulichkeit, Integrität und Verfügbarkeit unserer eigenen und uns anvertrauten Informationen und Daten zu gewährleisten und gegen interne und externe Bedrohungen zu schützen. Die siticom GmbH verpflichtet sich außerdem zur Aufrechterhaltung, Pflege und ständigen Weiterentwicklung seines Informationssicherheitsmanagementsystems (ISMS) nach dem ISO 27001 Standard. Dazu gehört auch die regelmäßige Sensibilisierung der Mitarbeiter für die Informationssicherheit und die informationssicherheitstechnische Kontrolle von Lieferanten.

Der Zweck dieser Leitlinie und somit der Informationssicherheit ist es, jederzeit sicherzustellen, dass der Schutz von Informationen der siticom GmbH, unseren Partnern und Kunden gegen interne und externe Bedrohungen – vorsätzlicher oder zufälliger Natur - stets gewährleistet ist.

Informationen sind in vielfältiger Art und Weise verfügbar und können unterschiedlich bedroht sein:
- Digitale Informationen - z.B. auf Festplatten/Harddisk (HD, HDD, SSD), Bändern, DVDs und USB-Sticks - können über Netzwerke und andere Wege einfach dupliziert und entwendet werden.
- Informationen in Papierform, ausgedruckt oder handschriftlich, können per Fax weitergeleitet oder kopiert werden.
- Mündliche Informationen, aus persönlichen Gesprächen oder Telefonaten können z.B. heimlich mitgehört und weitergegeben werden.

Das Ziel der Informationssicherheit der siticom GmbH ist darüber hinaus auch, die betriebliche Geschäftskontinuität zu gewährleisten. Dadurch werden potentiell auftretende Schäden für die siticom GmbH, unserer Partner und Kunden vermieden oder minimiert.

Zeitnahe und angemessene Korrekturen sowie Vorbeugungs- und Korrekturmaßnahmen sollen Sicherheitsvorfälle jeglicher Art möglichst vermeiden.

Um dies zu erreichen müssen

- wertvolle oder sensible Informationen vor unbefugtem Zugriff geschützt werden.
- die Richtigkeit und Vollständigkeit von Informationen vor unbefugter Änderung bewahrt werden.
- die Verfügbarkeit von Informationen und vitalen Diensten sichergestellt werden, sobald diese benötigt werden.

# 2 Leitlinie zur Informationssicherheit

## 2.1 Zielgruppe und Geltungsbereich

Das Informationssicherheitsmanagementsystem (im folgenden ISMS genannt) der siticom GmbH (im folgenden siticom genannt) besitzt Gültigkeit für alle Standorte des Unternehmens. Das ISMS ist fester Bestandteil des Integrierten Managementsystems (IMS, siehe Bild) der siticom.

Das ISMS besitzt Gültigkeit für alle aktuellen Niederlassungen der siticom.

Es umfasst die Vorgänge innerhalb der Räumlichkeiten der siticom, alle Aktivitäten von Mitarbeitern sowie auch direkt von der siticom beauftragte Dienstleister.

Der Anwendungsbereich des ISMS der siticom ist die

Geschäftskundenberatung für Entwicklung und Planung,
Einführung und Betrieb von Lösungen
sowie die Auswahl und Beschaffung von Technologien in den
Arbeitsgebieten IT-Infrastruktur, Sicherheit, Strategie, Organisation und Geschäftsprozessen.

## 2.2 Grundsätze der Informationssicherheit der siticom

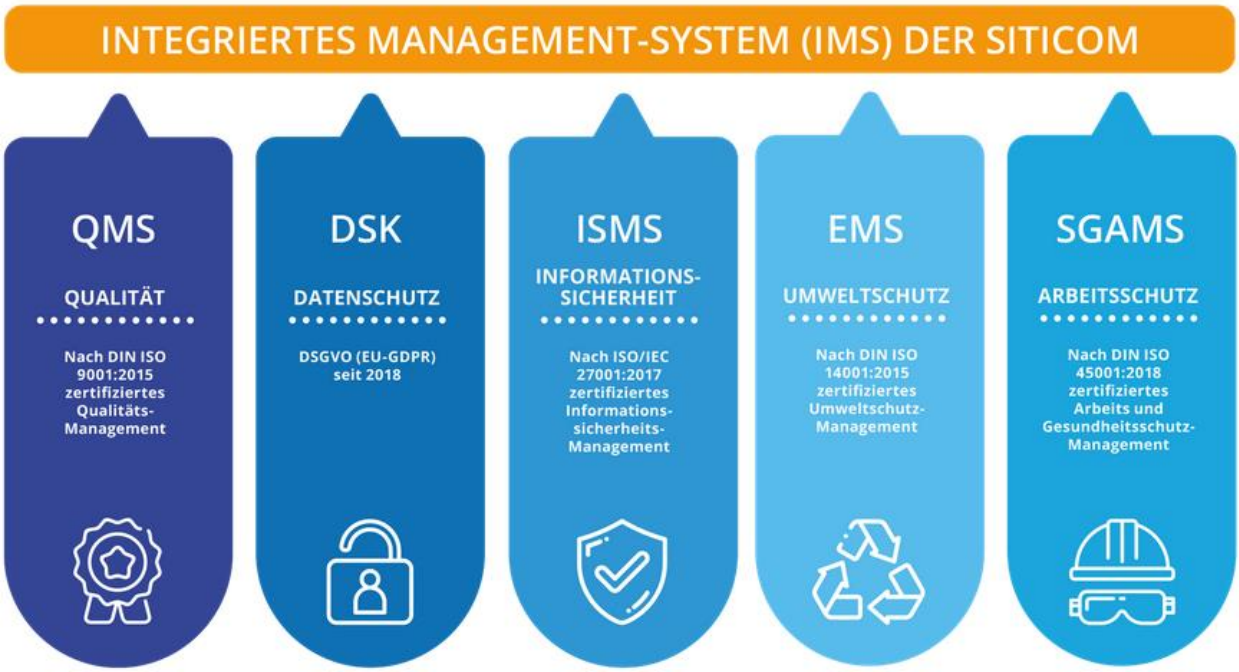
Das ISMS der siticom orientiert sich an folgenden Grundsätzen:

- Körperliche Unversehrtheit von Mitarbeitern und Drittparteien, sofern diese im Einflussbereich des Unternehmens tätig sind.
- Wahrung der Vertraulichkeit von Informationen der siticom sowie deren Geschäftspartner über alle Kommunikationsschnittstellen hinweg.
- Sicherstellung und Wahrung der Integrität und Verfügbarkeit von Informationen
- Aufrechterhaltung einer wirksamen betrieblichen Geschäftskontinuität der siticom
- Ständige Aufrechterhaltung und Erweiterung der Mitarbeiterkompetenz
- Aufrechterhaltung eines hohen Bewusstseins für Informationssicherheit in allen Bereichen der siticom
- Bekenntnis zur kontinuierlichen Verbesserung
- Aufrechterhaltung wirksamer Zugangskontrollen
- Erfüllung rechtlicher und vertraglicher Anforderungen
- Lernen aus Informationssicherheitszwischenfällen, egal ob diese tatsächlich eingetreten sind oder nur vermutet wurden
- Pflege eines wirksamen Risikomanagements

Die Anforderungen der Organisation (Business) sowie gesetzlicher Vorgaben zum Datenschutz aus dem BDSG sowie der entsprechenden europäischen Verordnung (EU-DSGVO) an Informationen und Informationssysteme werden jederzeit gewährleistet und sind mit dem strategischen und operativen Risikomanagement der siticom abgestimmt.

## 2.3 Das ISMS der siticom

Die Geschäftsführung der siticom GmbH verpflichtet sich zu einer kontinuierlichen Verbesserung des ISMS im Rahmen des existierenden Integrierten Managementsystems (IMS) und stellt die hierfür notwendigen Mittel und Ressourcen zur Verfügung.




Sie verpflichtet sich außerdem zur Einhaltung anwendbarer rechtlicher, vertraglicher und organisationseigener Vorgaben, um den Erwartungen interessierter Parteien an die Informationssicherheit auf einem hohen Stand zu entsprechen.

### 2.3.1 Anforderungen an die Mitarbeiter und Dienstleister der siticom

Alle Führungskräfte sind direkt verantwortlich für die Implementierung und Einhaltung der Grundsätze der Richtlinie zur Informationssicherheit innerhalb ihrer Organisationseinheiten.

Alle Führungskräfte stellen sicher, dass die Richtlinie zur Informationssicherheit ihren Mitarbeitern sowie relevanten Drittparteien bekannt ist und deren Grundsätze befolgt werden und die von ihnen abgeleiteten Informationssicherheitsziele in keinem Widerspruch dazu stehen.

Jeder Mitarbeiter ist verantwortlich für die Einhaltung der Grundsätze der Richtlinien zur Informationssicherheit.
Externe Dienstleister sind ebenfalls verantwortlich für die Einhaltung der Sicherheitsregeln zur Informationssicherheit. Das entsprechende Regelwerk dazu wird externen Dienstleistern zugänglich gemacht.

Nachgelagerte Richtlinien, Verfahrensanweisungen und Prozessbeschreibungen sind für alle Mitarbeiter verbindlich und stellen sicher, dass die Anforderungen an die Informationssicherheit sowie gesetzliche Anforderungen (z.B. die EU-Datenschutzgrundverordnung) angemessen erfüllt werden.

Ihnen ist daher in jedem Fall zu folgen. Sollte dies in begründeten Fällen nicht möglich sein, ist gemäß dem Prozess zum Umgang mit Sicherheitsvorfällen und Sicherheitsschwachstellen ein Sicherheitsvorfall mit der Begründung der Nichteinhaltung innerhalb von 24 Stunden zu dokumentieren, um den kontinuierlichen Verbesserungsprozess anzustoßen.

Vermutete oder erfolgte Verstöße gegen die Informationssicherheit (Sicherheitsvorfälle) sind gemäß der Prozessbeschreibung zum Umgang mit Sicherheitsvorfällen und Sicherheitsschwachstellen

umgehend, aber maximal innerhalb von 24 Stunden, zu melden. Das Nicht-Melden eines Sicherheitsvorfalls ist selbst ein meldepflichtiger Sicherheitsvorfall.

Bewusste oder fahrlässige Verstöße gegen die Informationssicherheit werden im Rahmen der arbeitsrechtlichen Bestimmungen behandelt.

Auf jeden Fall ist der Informationssicherheitsbeauftragte (ISB) um Rat zu fragen.

Das Erkennen, Melden und Dokumentieren von Sicherheitsvorfällen zum Datenschutz ist in der EU-Datenschutzgrundverordnung gesetzlich vorgeschrieben und hilft überdies, die Informationssicherheit im Rahmen unseres kontinuierlichen Verbesserungsprozesses weiter zu verbessern.

### 2.3.2 Lenkung von Dokumenten und Informationen

Organisationseigene Dokumentationen dienen der Sicherung der Wertschöpfung der siticom. Sie werden dabei stets unter dem Gesichtspunkt der Effektivität und Effizienz erstellt, gepflegt und aufbewahrt. Dabei sind in jedem Fall die Anforderungen an die Lenkung von Dokumenten und Informationen zu beachten.

### 2.3.3 Rollen und Verantwortlichkeiten

Das Management der Informationssicherheit wird durch den Informationssicherheitsbeauftragten (ISB) in der siticom wahrgenommen.

Der ISB ist verantwortlich für die Aktualisierung sowie für Hinweise zur Implementierung der Richtlinie zur Informationssicherheit sowie der nachgelagerten Richtlinien.

Für Fragen, Hinweise und Beobachtungen, die im Zusammenhang mit der Informationssicherheit der siticom stehen, können per Email: ISB@siticom.de an die Sicherheitsorganisation gerichtet werden. Die Kommunikation erfolgt dabei auf Wunsch vertraulich und stets unter Einhaltung der gesetzlichen Anforderungen.

# 3 Dokumente und Referenzen

| Abk. | Dokumentenidentifikation |
|---|---|
| BDSG | Bundesdatenschutzgesetz |
| EU-DSGVO | Europäische Datenschutzgrundverordnung |
| ISO 27001 | Die internationale Norm ISO/IEC 27001 Information Technology – Informationssicherheits-Managementsysteme – Anforderungen |

| ISO Kontrolle | Beschreibung |
|---|---|
| A.5.1.1 | Informationssicherheitsrichtlinien |
| A.5.1.2 | Überprüfung der Informationssicherheitsrichtlinien |