Leitlinien zur Informationssicherheit

Inhalt

1. Allgemeines 2
   1.1. Inhalt 2
   1.2. Zweck 2
   1.3. Geltungsbereich 2
2. Stellenwert der Informationssicherheit 3
   2.1. IT ist unverzichtbare Basis vieler Geschäftsprozesse 3
   2.2. Sicherheit als Grundlage des Geschäftes 3
   2.3. Erfüllung gesetzlicher und vertraglicher Verpflichtungen 3
   2.4. Erfüllung der Anforderungen von interessierten Parteien 3
   2.5. Bedeutung der Informationssicherheit 3
   2.6. Herkunft der Leitlinien 3
3. Informationssicherheitsziele und Schutzmaßnahmen 4
   3.1. Eigene Ziele 4
   3.2. Bedürfnisse und Anforderungen von interessierten Parteien 4
      3.2.1. Geschäftsführung 4
      3.2.2. Gesellschafter 4
      3.2.3. Geschäftspartner/Kunden/Endkunden 4
      3.2.4. Mitarbeiter 5
      3.2.5. Banken 5
      3.2.6. Aufsichtsbehörden 5
   3.3. Schutzziele 5
   3.4. Schutzmaßnahmen 5
   3.5. Gesetzliche Anforderungen 6
   3.6. Vertragliche Anforderungen 6
4. Organisationsstruktur und Verantwortlichkeit 7
5. Kontakt & Kommunikation 9
   5.1. Kontakt zu Behörden 9
   5.2. Kontakt zu Interessenvertretungen 9
   5.3. Sonstige Informationsquellen 9
   5.4. Kontakt zu Dritten 9
6. Sicherheitsbewusstsein aller Beteiligten 10
7. Überprüfung und Verbesserung 10
8. Schulungs- und Sensibilisierungsmaßnahmen 10
9. Sanktionen 10

1. Allgemeines

1.1. Inhalt

Inhalt dieser Richtlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für das Informationssicherheits-Management der Sikom Software GmbH.

1.2. Zweck

Der Zweck des Informationssicherheits-Managementsystems ist es das Unternehmen vor Risiken, die sich aus der Verarbeitung und Nutzung von Informationen ergeben, zu schützen, um den Fortbestand des Unternehmens, einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb **sicherzustellen**.

1.3. Geltungsbereich

Diese Richtlinie wird auf das gesamte Informationssicherheits-Managementsystem (ISMS) angewendet.

Das ISMS erstreckt sich auf den Unternehmenssitz der Sikom Software GmbH in Heidelberg, Tullastrasse 4, den Entwicklungsstandort in Zwickau, Herschelstrasse 27 und die im Rahmen von Projekten bei Kunden vor Ort oder im Home-Office arbeitenden Mitarbeiter.

Es erstreckt sich zudem auf alle Geschäftsprozesse des Unternehmens, und zwar auf:

- Entwicklung (Grundlagen- und Projektentwicklung),
- Projektmanagement,
- Produktmanagement,
- Technik/Support/TBO (IT-Infrastruktur, Support/TBO und Technische Kundenbetreuung),
- Qualitätssicherung (QS),
- Business Development (Einkauf, Finanzen, Marketing, Personal, Strategisches Consulting, BCS-Prozesse),
- ISMS und DSGVO,
- Vertrieb (Inside Sales und Sales Consulting),
- und alle dort tätigen internen und externen Mitarbeiter und Dienstleister.

Die Unternehmensstruktur ist im Dokument „M01_2 Sikom Orga BCS MA.pdf“ hinterlegt.

Die Informationssicherheitsleitlinien sind Aufforderung und Verpflichtung zu gesetzeskonformem Verhalten und verantwortungsbewusstem Umgang mit den Informationen und der IT-Infrastruktur der Sikom Software GmbH für alle, die diese Infrastruktur nutzen.

Sie werden allen Mitarbeitern, Partnern und ggf. weiteren Personen oder Einrichtungen in geeigneter Weise zur Kenntnis gegeben. Die Informationssicherheitsleitlinien sind bei allen Vorhaben zu berücksichtigen.

2. Stellenwert der Informationssicherheit

2.1. IT ist unverzichtbare Basis vieler Geschäftsprozesse

Die Sikom Software GmbH (Sikom) ist als ein führender Hersteller von Contact Center Lösungen auf die Verfügbarkeit moderner Informations- und Kommunikationstechnik angewiesen, um ihre Geschäftsprozesse durchzuführen und um mit ihren Kunden und Geschäftspartnern zusammenarbeiten zu können.

2.2. Sicherheit als Grundlage des Geschäftes

Das Vertrauen von Kunden, Partnern und Mitarbeitern in die Sicherheit, d.h., die *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* der Informationen ist Grundlage der Geschäftstätigkeit der Sikom. Ohne dieses Vertrauen wäre der Erfolg und der Fortbestand der Sikom nicht möglich.

2.3. Erfüllung gesetzlicher und vertraglicher Verpflichtungen

Darüber hinaus bestehen Verpflichtungen zur Gewährleistung der Informationssicherheit aufgrund gesetzlicher Bestimmungen und vertraglicher Verpflichtungen gegenüber Kunden, Mitarbeitern und Partnern.

2.4. Erfüllung der Anforderungen von interessierten Parteien

Wichtig für den dauerhaften Erfolg der Sikom ist es, die Anforderungen der Kunden und anderer relevanter interessierter Dritter an die Informationssicherheit zu berücksichtigen.

2.5. Bedeutung der Informationssicherheit

Dem Schutz der Informations- und Kommunikationsinfrastruktur der Sikom vor Missbrauch, Manipulation, Störungen sowie dem Schutz der gespeicherten und verarbeiteten Informationen vor Manipulation oder Ausspähen – kurz: der Informationssicherheit – kommt daher eine große Bedeutung zu.

2.6. Herkunft der Leitlinien

Aus diesem Grund hat die Geschäftsführung der Sikom gemeinsam mit den geschäftsführenden Gesellschaftern die nachstehenden Leitlinien für den Umgang mit der Informationstechnik der Sikom beschlossen.

3. Informationssicherheitsziele und Schutzmaßnahmen

3.1. Eigene Ziele

Die Ziele der Informationssicherheit orientieren sich an der Unternehmensstrategie und den Unternehmenszielen und dienen dazu, einen anhaltenden geschäftlichen Erfolg und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Daher erfolgt die Sicherstellung der Informationssicherheit im ureigenen Interesse der Sikom, aber auch im Sinne von deren Kunden, Mitarbeitern und Geschäftspartnern.

Im Detail beinhalteten die Ziele:

- **Kunden:**
  Wir schaffen laufend mit unseren Kunden sichere IT-Lösungen mit bestmöglichem Nutzen und größtmöglichen Maß an Sicherheit für unsere Kunden. Unser Anspruch ist dabei eine hohe Verfügbarkeit unserer Kundenanwendungen.
- **Verantwortung:**
  Wir übernehmen immer und fortwährend die Verantwortung für unser Handeln. Das beinhaltet auch die Einhaltung aller gesetzlichen Vorschriften und die kontinuierliche Anpassung an zukünftige Änderungen der gesetzlichen Vorgaben.
- **Vertrauen:**
  Wir wissen, dass für eine nachhaltige Partnerschaft und Zusammenarbeit Vertrauen die Grundlage bildet. Diese sichern wir, wenn wir die Vertraulichkeit und Integrität aller Kunden- und Unternehmensdaten durch Maßnahmen zur Informationssicherheit und zum Datenschutz sicherstellen.
- **Selbstverständnis:**
  Wir leben eine Sicherheitskultur in unserem Unternehmen. Dabei wollen wir möglichen Schäden möglichst früh und effektiv vorbeugen. Dazu ist unser Wissen immer auf dem neuesten Stand. Weiterbildung und Sensibilisierung treiben wir zudem voran. Bei der Gestaltung und der Durchführung unserer relevanten Geschäftsprozesse werden immer technische und organisatorische Maßnahmen zur Verfügbarkeit, Integrität und Vertraulichkeit aller Daten und Informationen identifiziert und deren Umsetzung sichergestellt. Unsere eigene Infrastruktur halten wir ebenfalls hochverfügbar.

3.2. Bedürfnisse und Anforderungen von interessierten Parteien

3.2.1. Geschäftsführung

Die Geschäftsführung möchte mit dem ISMS sicherstellen, dass andauernd ein angemessenes Sicherheitsniveau mit möglichst geringem Aufwand erreicht wird. Das ISMS soll die Sikom jetzt und in Zukunft

- effektiv,
- effizient und
- compliant

in Bezug auf die Informationssicherheit machen.

3.2.2. Gesellschafter

Die Gesellschafter erwarten eine angemessen hohe Informationssicherheit im Unternehmen, da dies eine wichtige Grundlage für die Stabilität des Unternehmens ist.

3.2.3. Geschäftspartner/Kunden/Endkunden

Die Geschäftspartner erwarten einen vertraulichen und allgemein sicheren Umgang mit ihren Daten sowie eine stabil funktionierende IT-Infrastruktur als Grundlage einer reibungslosen Zusammenarbeit. Dazu gehört auch die Fähigkeit, Abrechnungen termingerecht zu verarbeiten.

Es ist zudem besonders wichtig, dass der laufende Betrieb beim Kunden nicht gestört wird, Ausfallsicherheit und Hochverfügbarkeit sind Schlüsselelemente der Sikom Anwendungen.

3.2.4. Mitarbeiter

Die Mitarbeiter erwarten einen angemessenen Schutz ihrer persönlichen Daten sowie eine reibungslos funktionierende Infrastruktur. Darüber hinaus können die Mitarbeiter erwarten, über die Umsetzung der Sicherheitsmaßnahmen sowie die an sie gestellten Erwartungen umfassend informiert zu werden.

3.2.5. Banken

Die Banken erwarten eine angemessen hohe Informationssicherheit im Unternehmen, da dies eine wichtige Grundlage für die Stabilität des Unternehmens ist.

3.2.6. Aufsichtsbehörden

Das BSI und die Landesdatenschutzbehörde erwarten die Einhaltung aller gesetzlichen Vorschriften und die kontinuierliche Anpassung an zukünftige Änderungen der gesetzlichen Vorgaben.

3.3. Schutzziele

Um Beeinträchtigungen der Informationssicherheit zu minimieren, ist das Management von angemessenen Sicherheitsmaßnahmen unter Berücksichtigung einer großen Bandbreite von Bedrohungen erforderlich:

- Die Sikom schützt ihre eigene Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit.
- Die Sikom schützt die Vertraulichkeit der verarbeiteten und gespeicherten Daten ihrer Kunden, Geschäftspartner und Mitarbeiter.
- Die Sikom schützt vertrauliche Informationen wie z.B. Geschäftsprozesse, Vertragsdaten, den eigenen Quellcode oder sonstige Geschäftsgeheimnisse.
- Die Sikom gewährleistet die Verfügbarkeit ihrer IT-Systeme, Programme und Daten.
- Die Sikom schützt die Integrität ihrer IT-Systeme, Programme und Daten.
- Die Sikom verhindert den Missbrauch ihrer IT-Systeme, Programme und Daten oder deren zweckwidrige Nutzung bzw. die Nutzung durch Unbefugte.

3.4. Schutzmaßnahmen

Die Schutzmaßnahmen umfassen:

- technische Maßnahmen (Software, Hardware, Konfiguration),
- organisatorische Vorkehrungen (verbindliche Regeln und Vorgaben) und
- personelle Maßnahmen (Schulungen, Mitarbeiterauswahl).

Sie werden in

- dem Sicherheitshandbuch,
- verschiedenen Betriebshandbüchern und
- relevanten Arbeitsanweisungen (AAW)

hinterlegt und sind zu befolgen.

3.5. Gesetzliche Anforderungen

Eine Vielzahl gesetzlicher Anforderungen muss im Rahmen des Informationssicherheitsmanagements berücksichtigt werden. Die detaillierte Erfassung der anwendbaren gesetzlichen und regulatorischen Anforderungen sowie deren Änderung erfolgt durch die jeweiligen Verantwortlichen. Diese sind im Dokument *„M01_1 Gesetzliche Anforderungen.pdf“* dokumentiert. Die Kommunikation relevanter Anforderungen an die Mitarbeiter erfolgt durch Geschäftsführung Strategie, Projekte, HR & Finanzen und den ISB.

3.6. Vertragliche Anforderungen

Die vertraglichen Anforderungen hinsichtlich der Informationssicherheit ergeben sich aus

- Service- und Wartungsverträgen mit Kunden und Partnern,
- Auftragnehmer oder Auftraggeber AGB’s und/oder TOM‘s
- Projektverträgen und/oder Auftragsbestätigungen und
- Vertraulichkeitsvereinbarungen.

Die vertraglichen Anforderungen hinsichtlich der Informationssicherheit werden vom DSGVO-Koordinator/in erfasst. Die Kommunikation der Anforderungen erfolgt durch den ISB/DSB.

Sikom übernimmt keine Aufgaben im Rahmen der Auftragsdatenverarbeitung.

4. Organisationsstruktur und Verantwortlichkeit

Das Erreichen, Erhalten und ständige Verbessern eines angemessenen Sicherheitsniveaus erfordert ein kontinuierliches Engagement von allen mit der Informationsverarbeitung befassten Personen wie dem Management, den Nutzern, den Softwareentwicklern sowie den Administratoren und den Mitarbeitern der Qualitätssicherung.

- Die gesamte *Geschäftsführung* trägt die Gesamtverantwortung für die Informationssicherheit. Sie initiiert und koordiniert die entsprechenden Aktivitäten und sorgt für die nötige Priorität und Aufmerksamkeit für Fragen der Informationssicherheit. Die Geschäftsführung ist insbesondere verantwortlich für die organisatorische Verankerung von Aktivitäten zur Einrichtung, Erhaltung und Weiterentwicklung der Informationssicherheit sowie für die technische und personelle Ressourcen-Ausstattung für die Informationssicherheit und deren angemessene Einbettung in die Strukturen und die Hierarchie der Firma. Sie setzt die Leitlinien sowie die Richtlinien zur Informationssicherheit in Kraft, lässt sich regelmäßig über die Wirksamkeit des ISMS berichten und legt bei Bedarf Maßnahmen fest.
- Die *Informationssicherheitsbeauftragte* verantwortet die Dokumentation des ISMS, und führt Aufzeichnungen über Informationssicherheitsereignisse und Planungen zur Informationssicherheit. Sie ist Ansprechpartner für Geschäftsführung und Mitarbeiter in allen Fragen der Informationssicherheit. Sie berichtet direkt an die Geschäftsleitung.
- Der *Arbeitskreis Informationssicherheit* unterstützt die Geschäftsführung bei der unternehmensweiten Koordinierung und Lenkung der Informationssicherheitsmaßnahmen. Er erarbeitet konkrete Vorschläge technischer und organisatorischer Art zur Verbesserung der Informationssicherheit. Er hat darüber hinaus die Aufgabe, die bestehende Informationssicherheit zu bewerten, neue Gefahren zu erkennen und die einzelnen Sicherheitsmaßnahmen so zu koordinieren, dass ein angemessenes Sicherheitsniveau mit möglichst geringem Aufwand erreicht wird.
- Die *IT-Verantwortlichen* legen in Abstimmung mit dem Informationssicherheitsbeauftragten diejenigen Maßnahmen fest, die aus ihrer Sicht zur Verbesserung und Erhaltung der Sicherheit in ihrem jeweiligen Wirkungsbereich ergriffen werden müssen. Sie reagieren außerdem eigenverantwortlich bei Verstößen gegen die und bei Nichtbeachtung von Informationssicherheitsvorgaben.
- Die *Administratoren* setzen in enger Abstimmung mit dem jeweiligen IT-Verantwortlichen, bzw. Informationssicherheitsbeauftragten die notwendigen technischen und *organisatorischen Maßnahmen zur Absicherung der IT-Infrastruktur um. Sie erarbeiten konkrete Handlungsanweisungen für die Benutzer der IT-Infrastruktur auch in Bezug auf die Informationssicherheit* und sind aufgefordert, dem Arbeitskreis Informationssicherheit bzw. den IT-Verantwortlichen Vorschläge für die Verbesserung der Informationssicherheit zu unterbreiten. Die Handlungsanweisungen werden in einem S*icherheitshandbuch* gesammelt.
- Der *Datenschutzbeauftragte* (externe Datenschutzbeauftragte) ist das Kontrollorgan in allen Datenschutzfragen. Er wirkt auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. In Zusammenarbeit mit dem DSGVO-Koordinator/in, dem innerbetrieblichen Kontrollorgan in Datenschutzfragen, unterstützt er darüber hinaus die Leitung des Unternehmens sowie die Mitarbeiter bei der Identifikation von datenschutzrechtlichen Belangen sowie der Planung und Umsetzung von Maßnahmen zum Datenschutz
- Die *Vorgesetzten mit Personalverantwortung* stellen sicher, dass die getroffenen technischen, organisatorischen und personellen Maßnahmen zur Informationssicherheit in Bezug auf die ihnen unterstellten Mitarbeiter bzw. die in ihrem Verantwortungsbereich tätigen Nutzer umgesetzt werden. Sie überprüfen in regelmäßigen Abständen deren Einhaltung.
- Jeder *Mitarbeiter* trägt durch sein Verhalten zur Gewährleistung der Informationssicherheit bei. Er achtet darauf, Regelungen zur Informationssicherheit konsequent anzuwenden und Informationssicherheitsmaßnahmen umzusetzen. Er meldet Schwachstellen der Informationssicherheit, Ereignisse, mögliche Störungen, Sicherheitsvorfälle oder Notfälle umgehend. Zu diesem Zweck erhalten alle Mitarbeiter Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und ihren Sicherheitsmechanismen.

- Die *Software-Entwickler* achten bei der Programmierung neuer Anwendungen in besonderem Maß auf Informationssicherheitsaspekte um evtl. Schwachstellen der Informationssicherheit schon im Vorfeld zu vermeiden. Zu diesem Zweck erhalten sie Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und ihren Sicherheitsmechanismen.
- Die *Qualitätssicherung* überprüft Anwendungen in besonderem Maß die Informationssicherheitsaspekte, um evtl. Schwachstellen der Informationssicherheit schon im Vorfeld zu vermeiden. Zu diesem Zweck erhalten sie Informationen, Schulung und Betreuung im Umgang mit den IT-Systemen und ihren Sicherheitsmechanismen. Zudem kommen Qualitätssicherungsprozesse zum Einsatz und Protokolle werden diesbezüglich abgearbeitet.

5. Kontakt & Kommunikation

5.1. Kontakt zu Behörden

Kontaktperson	Behörde	Kontakt über
ISB / Stv. ISB	Allianz für Cybersicherheit	www.allianz-fuer-cybersicherheit.de
ISB / Stv. ISB	Landesbeauftragter für Datenschutz und Informationsfreiheit B-W	www.baden-wuerttemberg.datenschutz.de
ISB / Stv. ISB	Sächsischer Datenschutzbeauftragter	www.saechsdsb.de

5.2. Kontakt zu Interessenvertretungen

Kontaktperson	Interessensvertretung	Kontakt über
ISB / Stv. ISB	TeleTrusT	Newsletter
ISB / Stv. ISB	BitKOM	Newsletter

5.3. Sonstige Informationsquellen

Kontaktperson	Interessensvertretung	Kontakt über
ISB / Stv. ISB	Heise security	Newsletter
ISB / Stv. ISB	BSI IT-Grundschutz-Newsletter	Newsletter
ISB / Stv. ISB	BSI BürgerCERT Newsletter	Newsletter
ISB / Stv. ISB	Althammer & Kill	Newsletter
ISB / Stv. ISB	Datenschutz Guru	https://www.datenschutz-guru.de/
ISB / Stv. ISB	GDD e.V.	https://www.gdd.de/

5.4. Kontakt zu Dritten

Kontaktperson	Dritte	Kontakt über
Zuständiger Projektleiter	Kunden	Email, Telefon, Post
Vertrieb	Kunden	Email, Telefon, Post
ISB / DSB	Anfragen von Betroffenen	Email, Telefon, Post
Marketing	Anfragen von Interessenten	Email, Telefon, Post
Personal	Anfragen von Bewerbern	Email, Telefon, Post
Marketing	Anfragen von Medien	Email, Telefon, Post

6. Sicherheitsbewusstsein aller Beteiligten

Alle Mitarbeiter und Partner der Sikom verpflichten sich beim Umgang mit Informationen und Einrichtungen jederzeit aufmerksam die Belange der Informationssicherheit zu berücksichtigen.

Sofern sie Umstände erkennen, die möglicherweise auf eine Einschränkung der Informationssicherheit, auf eine Gefährdung der Informationssicherheit oder auf Verbesserungsmöglichkeiten hinweisen, so melden sie diese an den nächsten erreichbaren Vorgesetzten bzw. Ansprechpartner oder den Informationssicherheitsbeauftragten.

7. Überprüfung und Verbesserung

Die Erreichung und Verbesserung des angestrebten Sicherheits- und Datenschutzniveaus wird durch eine *kontinuierliche Revision* der Anforderungen, Regelungen und *Überprüfung* von deren Einhaltung bzw. *Messung* der Wirksamkeit der Maßnahmen sichergestellt.

Die Leitlinie zur Informationssicherheit wird in regelmäßigen Abständen auf ihre Aktualität und Wirksamkeit hin überprüft und gegebenenfalls angepasst. Im Besonderen wird die Leitlinie bei Änderungen der Bedrohungslage aufgrund aktueller Ereignisse oder der Einführung neuer Technologien in der Firma überprüft und angepasst. Unabhängig davon erfolgt eine Überarbeitung der Leitlinie *mindestens alle zwei Jahre*.

8. Schulungs- und Sensibilisierungsmaßnahmen

Die Geschäftsführung sowie die verantwortlichen Mitarbeiter der Firma stellen sicher, dass neu eingestellte Mitarbeiter ebenso wie bereits beschäftigte Mitarbeiter auf die Einhaltung der Leitlinien hingewiesen werden. In regelmäßigen Abständen werden die Mitarbeiter auf die Problematiken und Gefährdungen der Informationssicherheit hingewiesen. Mitarbeiter, die direkten Umgang mit sensiblen Informationen haben, werden in internen oder externen Schulungen mit den Gefahren und Maßnahmen der Informationssicherheit vertraut gemacht. Die Schulungen werden entsprechend dem Schulungskonzept sowie dem Schulungsplan vorgenommen.

9. Sanktionen

Die Geschäftsführung sowie Mitarbeiter mit Personalverantwortung stellen sicher, dass die Leitlinien zur Informationssicherheit durch alle Mitarbeiter befolgt werden. Mitarbeiter, die gegen diese Leitlinie verstoßen, können mit angemessenen Sanktionen belegt werden. Schwerwiegende Verstöße gegen die Grundsätze der Informationssicherheit können zu Abmahnung oder fristloser Kündigung eines Mitarbeiters führen.