SCHWARZWALD-BAAR
KLINIKUM

Leitlinie

Informations-Sicherheits-Management-System
Datenschutz-Management-System
Lieferanten

der Schwarzwald-Baar Klinikum Villingen-Schwenningen GmbH

Geschäftsführer: Dr. Matthias Geiser
Vorsitzender des Aufsichtsrates (alternierend):
Sven Hinterseh (Landrat)
Jürgen Roth, Oberbürgermeister

Sitz der Gesellschaft:
Villingen-Schwenningen
Registergericht: Reg.-Nr. HRB 602038
Amtsgericht Freiburg
KH-Kenn.-Nr.: IK 260 831 312

Bankverbindung
Sparkasse Schwarzwald_Baar
IBAN: DE49 69450065 0000 064220
BIC: SOLADES1VSS

Inhalt

Präambel

Der Zweck dieses Dokuments ist die Festlegung der Vorschriften für Beziehungen zu Lieferanten, Dienstleistern und Partnern (im Folgenden Lieferanten genannt.
Zum Erhalt der flüssigen Lesbarkeit des Textes wird bewusst auf die genderkorrekte Schreibweise verzichtet und in der Regel die maskuline Schreibweise gewählt.

1. Stellenwert der Informationssicherheit und des Datenschutzes

Die stetige steigende Unterstützung aller medizinischen und nichtmedizinischen Prozesse durch die Informationstechnologie geht mit einer ebenfalls steigenden Abhängigkeit von dieser Unterstützung einher.

Besondere Bedeutung kommt in unserem Klinikum den Schutzzielen Patientensicherheit und Behandlungseffektivität zu.

Patientensicherheit: Es ist sicherzustellen, dass die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen gewährleistet ist. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

Behandlungseffektivität: Es ist sicherzustellen, dass die Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen erfolgt.

Diese können nur dann gewahrt werden, wenn die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen sowie die Authentizität von Kommunikationspartnern richtig umgesetzt werden.

Integrität: Es ist sicherzustellen, dass Daten und Informationen während der gesamten Verarbeitung unversehrt, vollständig und aktuell bleiben.

Verfügbarkeit: Es ist sicherzustellen, dass Daten und Informationen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Vertraulichkeit: Es ist sicherzustellen, dass nur Befugte Daten und Informationen zur Kenntnis nehmen können.

Im Rahmen der Informationssicherheit wird auch den besonderen Datenschutzanforderungen Rechnung getragen. Die gesetzlichen Anforderungen der EU-Datenschutzgrundverordnung sowie die landes- und spezialrechtlichen Regelung fordern im Rahmen der Verarbeitung von personenbezogenen Daten besondere Schutzmaßnahmen zur Wahrung der Persönlichkeits- und Freiheitsrechte.

2. Weitere Ziele

Über die oben genannten Schutzziele hinaus verbindet das Klinikum mit den Aufgaben Informationssicherheit und Datenschutz folgende Ziele:

- Nachvollziehbarkeit und Rechtmäßigkeit der Datenverarbeitung
- Reduzierung von aus dem Betrieb von IT-Systemen entstehenden Risiken
- Erfüllung der gesetzlichen Anforderungen (DSGVO, BSIG, etc.)
- Einleitung und Umsetzung sicherheitsfördernder Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung
- Risikominimierung bei der Einführung neuer Technologien
- Vermeidung von Patientengefährdung durch IT-bedingte Störungen
- Wahrung der Schutzrechte von Betroffenen
- Umsetzung von Transparenz-, Informations- und Meldepflichten

3. Geltungsbereich

Dieses Dokument gilt für alle Mitarbeitenden, Dienstleister und Lieferanten, welche im und für den Anwendungsbereich des ISMS des Schwarzwald-Baar Klinikums tätig sind.

4. Verantwortlichkeit Informationssicherheit und Datenschutz

Die Geschäftsführung der SBK hat einen Informationssicherheitsbeauftragten (ISB) und einen Datenschutzbeauftragten (DSB) ernannt. Diese sind für die Belange der Informationssicherheit und des Datenschutzes innerhalb der SBK zuständig. Der Lieferant ist für alle Belange der Informationssicherheit und des Datenschutzes verantwortlich, die sich auf seine Geschäftsbeziehung mit der SBK auswirken bzw. direkten Einfluss haben. Lieferanten der SBK sind angehalten, sich konform zu der Informationssicherheits- / Datenschutzleitlinie der SBK und den Anforderungen dieser Richtlinie und allen daraus abgeleiteten Sicherheitsanweisungen zu halten. Die Ansprechpartner innerhalb der SBK werden dem Lieferanten im Rahmen der Vertragsbeziehung genannt und stehen als Ansprechpartner für Fragen zum ISMS / DSMS zur Verfügung.

5. Grundsätzliche Anforderungen an Lieferanten

1. Der Lieferant oder Dienstleister des SBKs verpflichtet sich bei Ausführung seines Auftrages zur Einhaltung aller einschlägigen Vorschriften, Normen, Verordnungen und Gesetze sowie der allgemein anerkannten Regeln der Technik. Er sichert zu, auch seine Subunternehmer sowie von diesen eingesetzten weiteren Auftragnehmern entsprechend zu verpflichten.

2. Der Lieferant ist insbesondere zur Einhaltung der datenschutzrechtlichen Bestimmungen verpflichtet. Er hat seine Mitarbeiter und von ihm beauftragte Subunternehmer auf die gesetzlichen Vorschriften zum Datenschutz hinzuweisen und zu verpflichten. Auf Nachfrage sind dem SBK die Verpflichtungen nachzuweisen.

3. Es besteht das Recht des SBKs auf Auskunft über die beim Lieferanten/Partner gespeicherten oder verarbeiteten Information.

4. Der Lieferant stellt sicher, dass seine Mitarbeiter und Subunternehmer Kenntnis von den wichtigsten Sicherheitsrichtlinien und Verfahrensanweisungen des SBKs haben und diese Regelungen einhalten.

6. Mitarbeiter des Lieferanten im Rahmen des ISMS / DSMS

1. Unterzeichnung des Dokumentes „Verpflichtungserklärung für Externe zur Wahrung der Vertraulichkeit, zur Beachtung des Datenschutzes und zur Wahrung von Geschäftsgeheimnissen“, soweit nicht bereits im Rahmen vertraglicher Regelungen mit dem Lieferanten (z.B. AV-Vertrag) geregelt.

2. Melden von Informationssicherheitsvorfällen / Schwachstellen / Datenschutzvorfällen (siehe Kapitel 7).

3. IT-Geräte, Dokumente, Informationen usw., die des SBKs dem Lieferanten zur Verfügung stellt, bleiben Eigentum des SBKs.

4. Die Informationen und Daten auf/in den genannten Geräten und Dokumenten unterliegen ausnahmslos der Schweigepflicht. Das gleiche gilt für alle Informationen und Daten, von denen der Lieferant im Zuge der Umsetzung eines Vertrags möglicherweise Kenntnis erlangt.

5. Der Austausch von (sensiblen) Daten erfolgt durch die vom SBK zur Verfügung gestellten Plattform.

6. Datenschutzrelevante Dokumente müssen ordnungsgemäß der Vorgaben des Datenschutzes entsorgt werden.

7. Informationssicherheits- / Datenschutzmeldungen

Verstöße gegen die Informationssicherheit bzw. den Datenschutz sind an folgende E-Mail-Adresse zu senden: datenpanne@sbk-vs.de
Der Lieferant muss seinen Ansprechpartner im SBK über sämtliche Probleme oder Alarme im Hinblick auf einen bestätigten oder vermuteten Verstoß gegen die Sicherheitsregeln zeitnah informieren.

8. Verschlüsselung

Daten mit einem erhöhten Schutzbedarf, wie z.B. personenbezogene Daten, Gesundheitsdaten oder vertrauliche Daten, dürfen per E-Mail oder per Datenträger außerhalb des hausinternen Netzwerkes des SBKs nur verschlüsselt (via S/MIME oder vergleichbare Verfahren) weitergegeben werden. Eventuelle Passwörter oder Schlüssel sind über einen anderen Kommunikationsweg als die Daten zu versenden.

9. Verhalten im Gebäude des SBKs

Die Registrierung und Einweisung von Dienstleistern und Lieferanten für die informationssicherheitsrelevanten Bereiche mit Zutrittsberechtigungen erfolgt über den Fachverantwortlichen des Bereiches des SBKs. Jeder Lieferant ist verpflichtet, die Sicherheitszonen innerhalb des SBKs zu wahren. Das Betreten von Bereichen nicht erteilter Zutrittsberechtigung ist untersagt. Unberechtigten Dritten ist der Zutritt zu verwehren. Die Türen zwischen den Sicherheitsbereichen sind immer ordnungsgemäß zu schließen (kein Blockieren).

10. Auditierung von Lieferantendienstleistungen

Das SBK ist dazu verpflichtet, die Einhaltung der Informationssicherheit und des Datenschutzes bei ihren Lieferanten zu überprüfen und zu bewerten. Das SBK behält sich vor, die Leistungen der Lieferanten nach vorheriger Abstimmung per Audit zu überprüfen. Ein Sicherheitsaudit kann jeden sicherheitsrelevanten Bereich abdecken, z. B. physische Sicherheit, logische Sicherheit, die Sicherheitsorganisation oder Sicherheitsverfahren. Zur Durchführung dieser Audits kann das SBK auch externe Dienstleister beauftragen. Sicherheitsaudits müssen im Ergebnis zu Empfehlungen und Maßnahmenplänen führen.