

Dokument-Nr.: ISB-ISMS-32149-00-MU  
Gültig seit: 31.05.2023  
Nächste Prüfung: 31.05.2025  
Dokumentenart: Mitgeltende Unterlagen

# InformationenSicherheitsManagementSystem

## Informationssicherheitsleitlinie für Vertragspartner des UKB

ISB-ISMS-32149-00-MU

Klassifizierung	OFFEN
Dokumenttyp	Mitgeltende Unterlagen
Version	1.1
Gültigkeit seit	31.05.2023
Nächste Prüfung	31.05.2025
Speicherort	myQM und ukbonn.de
Status	Freigegeben
Freigeber	Informationssicherheitsbeauftragter
Freigabe-Datum	31.05.2023

**Inhalt**

Versionshistorie ..... 2

1. Präambel ..... 3

    1.1. Übergeordnete Ziele ..... 3

    1.2. Anwendungsbereich und Anwender ..... 3

2. Erklärung zum Konsens bzgl. der Einhaltung von gesetzlichen Vorgaben..... 3

3. Vorgaben resultierend aus gesetzlichen Anforderungen für Vertragspartner des UKB ..... 3

    3.1. Allgemeine Vorgaben ..... 3

    3.2. Fernwartungsverträge..... 4

    3.3. Kauf- und Miet-/Leasing-Verträge für Informationstechnik, Kommunikationstechnik und Medizintechnik... 4

    3.4. Reparaturvertrag für Informationstechnik, Kommunikationstechnik und Medizinprodukte, die Datenträger  
enthalten. .... 4

## Versionshistorie

Version	Änderungen	Autoren	Datum
1.0	» Initiale Version	Peter Weidenbach	27.05.2019
1.1	» Anpassung an neues einheitliches ISMS Richtlinien Layout » Anpassung der geregelten B3S- Anforderungen an neue Nummerierungskonvention der B3S-Version 1.2 » Redaktionelle Überarbeitung	Tim Tang, Peter Weidenbach	09.03.2023

## 1. Präambel

Das Universitätsklinikum Bonn (UKB) ist gemäß IT-Sicherheitsgesetz und KRITIS-Verordnung eine Kritische Infrastruktur und daraus ergeben sich besondere Anforderungen an Informationssicherheit und Datenschutz, die auch Dienstleister, Hersteller und Lieferanten des Universitätsklinikums Bonn betreffen. Diese Leitlinie legt das gemeinsame Grundverständnis und den Stellenwert der Informationssicherheit und des Datenschutzes des UKB und der Vertragspartner des UKB dar. Diese Leitlinie ist Bestandteil der AGB des UKB und mit Abschluss des Vertrages bekennen sich die Vertragspartner zu dieser Leitlinie.

### 1.1. Übergeordnete Ziele

Die Vertragspartner bekennen sich zu den folgenden Zielen des UKB. Wenn im Einzelfall die Erfüllung aller Ziele nicht möglich ist, sind diese in absteigender Priorität (1 = Höchste Priorität) zu behandeln:

1. **Patientensicherheit** und **Behandlungseffektivität** dürfen nicht durch Informationssicherheitsvorfälle gefährdet werden.
2. Die **Verfügbarkeit** kritischer Dienstleistungen des UKB gemäß KRITIS-Verordnung ist jederzeit sicherzustellen.
3. Die **Vertraulichkeit** und **Integrität** personenbezogener Daten und insbesondere hochsensibler Patientendaten muss jederzeit gewährleistet sein.
4. Maßnahmen zur Informationssicherheit und Datenschutz müssen die **Einhaltung gesetzlicher Vorgaben** unter Wahrung einer **wirtschaftlichen Verhältnismäßigkeit** sicherstellen.

### 1.2. Anwendungsbereich und Anwender

Diese Leitlinie gilt für alle Verträge des UKB mit Dienstleistern, Herstellern und Lieferanten von Informationstechnik, Kommunikationstechnik und Medizintechnik, die die Patientenversorgung direkt oder indirekt tangieren. Sie gilt nicht für Verträge, die ausschließlich Forschung und Lehre betreffen oder keinen direkten oder indirekten Bezug zu Patienten bzw. Probanden haben.

## 2. Erklärung zum Konsens bzgl. der Einhaltung von gesetzlichen Vorgaben

Die Vertragspartner sind sich einig, dass alle gesetzlichen Vorgaben zum Thema Informationssicherheit und Datenschutz bei der Erfüllung des Vertrages eingehalten werden. Dies impliziert insbesondere, dass Produkte, die dem UKB angeboten werden, eine gesetzeskonforme Verwendung bzw. Betrieb für den am UKB vorgesehenen Einsatzzweck erlauben. Für den Bereich Informationssicherheit sind dies die Vorgaben aus dem Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus in Version 1.2 (B3S). Bzgl. des Datenschutzes finden die DSGVO, die Datenschutzgesetze des Landes Nordrhein-Westfalen, sowie §203 Strafgesetzbuch Anwendung.

## 3. Vorgaben resultierend aus gesetzlichen Anforderungen für Vertragspartner des UKB

Dieser Abschnitt listet Vorgaben für Vertragspartner des UKB auf, die aus den zuvor beschriebenen gesetzlichen Anforderungen resultieren. Der Abschnitt ist unterteilt in allgemeine Vorgaben und Vorgaben für bestimmte Arten von Verträgen. Diese Vorgaben dienen als Orientierung und haben keinen Anspruch auf Vollständigkeit.

### 3.1. Allgemeine Vorgaben

- » DSGVO: Wenn der Vertragspartner im Rahmen seiner Vertragspflichten mit personenbezogenen und insbesondere Patientendaten in Berührung kommt, muss ein Auftragsverarbeitungsvertrag (AVV) geschlossen werden.
- » B3S ANF-0071, DSGVO: Auftragnehmer sind dazu verpflichtet, Verstöße gegen die Informationssicherheit und den Datenschutz, die im Rahmen der Vertragserfüllung auffallen, zu melden. Die Meldung soll an den/die Datenschutzbeauftragte\*n des UKB erfolgen: [datenschutz@ukbonn.de](mailto:datenschutz@ukbonn.de)
- » B3S ANF-0093: Für den Austausch vertraulicher Daten muss im Vorfeld ein Übertragungsweg zwischen den Vertragspartnern abgestimmt werden, der einen angemessenen Schutz der Daten sicherstellt. Bei einer elektronischen Übertragung sind die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) anzuwenden. Dies gilt insbesondere für den Austausch sensibler personenbezogener Daten.

### **3.2. Fernwartungsverträge**

- » B3S ANF-0101: Im Vorfeld muss geklärt werden, wie Fernwartungszugriffe nachvollziehbar protokolliert werden.
- » B3S ANF-0102-0104: Im Vorfeld muss die technische Umsetzung der Fernwartung abgestimmt werden. Dieser muss nach Stand der Technik durch Verschlüsselung und Authentifizierung gesichert sein. Die Fernwartungsverbindung muss nach vollzogener Wartung trennbar sein.

### **3.3. Kauf- und Miet-/Leasing-Verträge für Informationstechnik, Kommunikationstechnik und Medizintechnik.**

- » B3S ANF-0148: Das UKB stellt dem Vertragspartner eine Liste mit technischen Mindestanforderungen bzgl. Informationssicherheit und Datensicherheit zur Verfügung. Diese Anforderungen sollen sicherstellen, dass ein wirtschaftlicher und gesetzeskonformer Betrieb der Geräte am UKB möglich ist. Der Vertragspartner muss prüfen, ob das angebotene Produkt alle jeweils relevanten Mindestanforderungen erfüllt und dies dem UKB mitteilen, bevor der Kaufvertrag abgeschlossen wird.
- » B3S ANF-0151: Bei der Beschaffung netzwerkfähiger Medizinprodukte muss der Vertragspartner notwendige Information für eine Risikobewertung gemäß DIN EN 80001 dem UKB im Vorfeld zur Verfügung stellen.
- » B3S ANF-0169-0170: Bei Miet- und Leasingverträgen muss die Löschung möglicher Patientendaten auf dem Medizinprodukt bzw. dem IT-System im Vorfeld geregelt werden. Die Löschung muss nach Empfehlungen des BSI erfolgen.

### **3.4. Reparaturvertrag für Informationstechnik, Kommunikationstechnik und Medizinprodukte, die Datenträger enthalten.**

- » B3S ANF-0170: Der Datenschutz bei Reparaturaufträgen ist im Vorfeld vertraglich zu regeln. Dies schließt insbesondere die gesetzeskonforme Entsorgung von Datenträgern mit ein, sofern diese ausgetauscht werden müssen.