

ISMS nach B3S

Kombiniertes Managementsystem für Cybersicherheit, Datenschutz in Krankenhäusern

(Kompatibel mit § 75c SGB V

<u>Anwendungshinweise</u>	6
<u>Vorwort</u>	6
<u>1.1 Die Anforderungen nach § 75c SGB V</u>	7
<u>1.2 Die Entwicklung der KRITIS Anforderungen für Krankenhäuser</u>	7
<u>1.3 IT-Sicherheitsgesetz</u>	7
<u>2 Methodik zur Erstellung des B3S</u>	9
<u>3 Branchenspezifischer Sicherheitsstandard (B3S) für die medizinische Versorgung nach DKG</u>	10
<u>3.1 Grundlegendes zur Anwendung des B3S</u>	10
<u>3.2 Anforderungen an Betreiber Kritischer Infrastrukturen</u>	11
<u>3.2.1 Maßnahmen zur Aufrechterhaltung des Versorgungsniveaus</u>	11
<u>3.2.2 Einrichten einer Kontaktstelle für das BSI</u>	11
<u>3.2.3 Aufbau von Meldeprozessen für Störungen oder Ausfälle an das BSI</u> ..	11
<u>3.3 Empfohlene Schritte zur Umsetzung des B3S</u>	12
<u>3.4 Deklaration von Anforderungen innerhalb des B3S</u>	14
<u>3.5 Definition der Schutzziele des B3S</u>	14
<u>3.6 Fortschreibung des B3S</u>	15
<u>4 Risikomanagement in der Informationssicherheit</u>	15
<u>4.1 Standard-Risikomanagement-Prozessmodell</u>	16
<u>4.2 Management-Anforderungen für die Implementierung eines Informationsrisikomanagement</u>	16
<u>4.2.1 Ermittlung der Risikoobjekte und Risiko-Eigentümer</u>	18
<u>4.2.2 Festlegung von Kritikalität</u>	18
<u>4.2.3 Risikoidentifikation</u>	20
<u>4.2.4 Risikobewertung</u>	20
<u>4.2.5 Risikobehandlung</u>	22
<u>4.2.6 Risikokommunikation und -überwachung</u>	23
<u>4.3 IT-Systemlandschaft in Krankenhäusern nach Kritikalität</u>	24

4.3.1	<u>Systeme der Klasse 1</u>	24
4.3.2	<u>Systeme der Klasse 2</u>	25
4.3.3	<u>Systeme der Klasse 3</u>	25
5	<u>Allgemeine Hinweise zur Definition des Geltungsbereichs</u>	25
5.1	<u>Branchenspezifischer Geltungsbereich</u>	26
5.2	<u>Ergänzende Regelungen zum Geltungsbereich</u>	27
5.2.1	<u>Übersicht der Kernprozesse und Funktionszuordnung innerhalb des Geltungsbereich</u>	27
5.2.1.1	<u>Vorbereitung / Aufnahme</u>	28
5.2.1.2	<u>Diagnostik</u>	29
5.2.1.3	<u>Therapie</u>	30
5.2.1.4	<u>Unterbringung und Pflege</u>	30
5.2.1.5	<u>Entlassung</u>	31
5.2.2	<u>Technische Unterstützungsprozesse in der stationären Versorgung</u>	31
5.2.2.1	<u>Informationstechnik (IT)</u>	32
5.2.2.2	<u>Kommunikationstechnik (KT)</u>	33
5.2.2.3	<u>Medizintechnik (MT)</u>	34
5.2.2.4	<u>Versorgungstechnik (VT)</u>	36
5.2.3	<u>Kritische branchenspezifische Anwendungssysteme</u>	37
5.2.3.1	<u>Krankenhausinformationssystem (KIS)</u>	37
5.2.3.2	<u>Laborinformationssystem (LIS)</u>	38
5.2.3.3	<u>Radiologieinformationssystem (RIS)</u>	38
5.2.3.4	<u>Picture Archive and Communication System (PACS)</u>	39
5.2.3.5	<u>Dokumenten-Management-System (DMS/ECM)</u>	39
5.2.3.6	<u>OP-Planungssystem</u>	40
5.2.3.7	<u>Systeme für Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)</u>	40
5.2.3.8	<u>Systeme der Versorgungstechnik</u>	40
5.2.3.9	<u>Systeme der Versorgungsdienste</u>	41
5.2.3.10	<u>Medizintechnik/-produkte</u>	41
5.2.3.11	<u>Spezialisierte Anwendungen im klinischen Umfeld</u>	42
5.3	<u>Festlegung der spezifischen Ziele und Anforderungen des B3S an die Informationssicherheit</u>	42
5.4	<u>Leitlinie zur Informationssicherheit</u>	43
6	<u>Branchenspezifische Gefährdungslage</u>	44
6.1	<u>Bedrohungsszenarien</u>	46

6.1.1	<u>Allgemeine Bedrohungen</u>	46
6.1.2	<u>IT-spezifische Bedrohungen</u>	46
6.2	<u>Schwachstellen</u>	47
6.3	<u>Branchenspezifische Gefährdungen</u>	47
6.4	<u>Gefährdungen kritischer branchenspezifischer Technik und Software</u>	48
6.4.1	<u>Krankenhausinformationssystem (KIS)</u>	48
6.4.2	<u>Laborinformationssystem (LIS)</u>	49
6.4.3	<u>Radiologieinformationssystem (RIS)</u>	50
6.4.4	<u>Picture Archive and Communication System (PACS)</u>	50
6.4.5	<u>Dokumenten-Management-System / Enterprise-Content-Management</u> 51	
6.4.6	<u>Medizintechnik</u>	51
6.4.7	<u>Transportlogistik</u>	52
6.4.8	<u>Versorgungstechnik</u>	52
6.4.9	<u>Versorgungsdienste</u>	52
6.4.10	<u>Sonder- und Spezial-Softwarelösungen</u>	53
6.5	<u>kDL-relevante IT-Systeme und Komponenten</u>	53
6.5.1	<u>Informationstechnik</u>	53
6.5.2	<u>Kommunikationstechnik</u>	54
6.5.3	<u>Versorgungstechnik</u>	54
6.5.4	<u>Medizintechnik/-produkte</u>	54
6.5.5	<u>Kritische branchenspezifische Anwendungssysteme</u>	55
7	<u>Anforderungen und Maßnahme Empfehlungen zur Umsetzung</u>	55
7.1	<u>Informationssicherheitsmanagementsystem (ISMS)</u>	56
7.2	<u>Organisation der Informationssicherheit</u>	56
7.2.1	<u>Geschäftsführung / Leitung</u>	57
7.2.2	<u>Beauftragter für Informationssicherheit (ISB, CISO)</u>	58
7.2.3	<u>Prozess- /Anwendungsverantwortlicher</u>	60
7.3	<u>Meldepflichten nach § 8b Absatz 4 BSI-Gesetz</u>	61
7.4	<u>Betriebliches Kontinuitätsmanagement</u>	61
7.5	<u>Asset Management</u>	63
7.6	<u>Robuste/resiliente Architektur</u>	64
7.7	<u>Physische Sicherheit</u>	65
7.8	<u>Personelle und organisatorische Sicherheit</u>	65
7.9	<u>Vorfallerkennung und Behandlung</u>	66
7.10	<u>Überprüfungen im laufenden Betrieb</u>	67
7.11	<u>Externe Informationsversorgung und Unterstützung</u>	68

<u>7.12</u>	<u>Lieferanten, Dienstleister und Dritte</u>	69
<u>7.13</u>	<u>Technische Informationssicherheit</u>	69
<u>7.13.1</u>	<u>Netz- und Systemmanagement (Netztrennung und Segmentierung)</u>	69
<u>7.13.2</u>	<u>Absicherung Fernzugriffe</u>	70
<u>7.13.3</u>	<u>Härtung und sichere Basiskonfiguration der Systeme und Anwendungen</u>	70
<u>7.13.4</u>	<u>Schutz vor Schadsoftware</u>	70
<u>7.13.5</u>	<u>Intrusion Detection / Prevention</u>	71
<u>7.13.6</u>	<u>Identitäts- und Rechtemanagement</u>	71
<u>7.13.7</u>	<u>Sichere Authentisierung</u>	72
<u>7.13.8</u>	<u>Kryptographische Absicherung (data in rest, data in motion)</u>	73
<u>7.13.9</u>	<u>Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. „bring your own device“ BYOD)</u>	73
<u>7.13.10</u>	<u>Vernetzung von Medizingeräten</u>	74
<u>7.13.11</u>	<u>Datensicherung, Datenwiederherstellung und Archivierung</u>	75
<u>7.13.12</u>	<u>Ordnungsgemäße Systemadministration</u>	75
<u>7.13.13</u>	<u>Patch- und Änderungsmanagement</u>	76
<u>7.13.14</u>	<u>Beschaffungsprozesse</u>	76
<u>7.13.15</u>	<u>Protokollierung</u>	77
<u>7.13.16</u>	<u>Umgang mit Datenträgern, Austausch von Datenträgern</u>	78
<u>7.13.17</u>	<u>Sicheres Löschen und Entsorgung von Datenträgern</u>	79