KASSENÄRZTLICHE
BUNDESVEREINIGUNG

RICHTLINIE - INFORMATIONSSICHERHEIT

KBV_ISMS_RL_ISP

DEZERNAT DIGITALISIERUNG UND IT

NIKO HILGENFELDT

22. OKTOBER 2019

1.12

INHALT

DOKUMENTENLENKUNG

Dokumententyp:	Richtlinie
Editor:	Niko Hilgenfeldt
Editiert am:	22.10.2019
Prüfer:	Sarah Schuchardt
Geprüft am:	23.10.2019
Freigeber:	Niko Hilgenfeldt
Freigegeben am:	30.10.2019
Version:	1.12
Status:	In Kraft

DOKUMENTENSTATUS

Version	Datum	Autor	Änderung	Begründung	Seite
1.12	22.10.2019	N. Hilgenfeldt	Anpassung Verteiler / Verteilerdienst	Organisationsveränderungen	5
1.11	04.10.2018	N. Hilgenfeldt	Definition des Anwendungsbereiches Überführung der Inhalte in das neue Corporate Design der KBV	Hinweise aus dem Überwachungsaudit 2017	8
1.10	10.11.2017	N. Hilgenfeldt	Dokumentenreview `17	Definition eines neuen Anwendungsbereiches und Organisationsveränderungen	
1.9	24.10.2016	N. Hilgenfeldt	Dokumentenreview `16	Umstellung der referenzierten ISMS-Dokumente	
1.8	26.02.2015	N. Hilgenfeldt	Dokumentenreview `15	Umstellung von ISO/IEC 27001/2005 auf ISO/IEC 27001:2013	
1.7	09.09.2014	N. Hilgenfeldt	Dokumentenreview `14	Organisationsveränderungen	
1.6	26.08.2013	N. Hilgenfeldt	Dokumentenreview `13 Kapitel 1.3 und Kapitel 1.4 geändert	Organisationsveränderungen	4, 5, 6, 9, 10,

Version	Datum	Autor	Änderung	Begründung	Seite
					11, 13
1.5	20.09.2012	J. Stein	Wechsel im Vorstand Kapitel zur Dokumentenlenkung erweitert.	Review 2012	
1.4	18.01.2011	J. Stein	Dokumentenreview 2011	Hinweise aus Audit etc.	
1.3	23.09.2010	S. Berger	Anpassung des Geltungsbereiches dieser Richtlinie Referenzierung auf die ISO 27002, Kapitel 5.1.1 sowie Verweis auf Maßnahmen der ISO 27001 in Kapitel 2.3	Hinweise aus ISMS-Assessment	4 8
1.2	10.05.2010	S. Berger	Redaktionelle Anpassungen		
1.1	05.05.2010	S. Berger	Strukturelle Anpassung sowie Einarbeitung von Hinweisen der Rechtsabteilung	Hinweise der Rechtsabteilung	
1.0	12.04.2010	S. Berger	Redaktionelle Anpassungen		
0.9	03.03.2010	S. Berger	Redaktionelle Anpassungen		
0.2	29.01.2010	S. Berger	Anpassung der referenzierten ISMS-Dokumente	Zusammenfassung von Richtlinien	
0.1	10.12.2009	S. Berger	Erstellung des Dokuments		

1. ALLGEMEINES

1.1 ZIEL DES DOKUMENTS

Dieses Dokument beschreibt die Richtlinie für die Informationssicherheit des Informationssicherheitsmanagementsystems (ISMS) im geltenden Anwendungsbereich [KBV_ISMS_RL_AWB] und damit die Informationssicherheitsziele der Kassenärztlichen Bundesvereinigung (KBV).

Ziel der vorliegenden Richtlinie ist die Richtungsvorgabe und Unterstützung durch den Vorstand der KBV bei der Informationssicherheit in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen. Der Vorstand der KBV gibt eine klare Richtung der Grundsätze in Einklang mit den Geschäftszielen vor. Er unterstützt und engagiert sich für Informationssicherheit durch die organisationsweite Veröffentlichung und Aufrechterhaltung dieser und weiterer ISMS-Richtlinien.

1.2 GELTUNGSBEREICH UND INKRAFTSETZUNG DES DOKUMENTS

Dieses Dokument gilt im Anwendungsbereich des ISMS der Kassenärztlichen Bundesvereinigung, das heißt für alle angestellten Mitarbeitenden und Auftragnehmer der KBV sowie sonstige externe Dritte, die Einrichtungen oder Informationen der KBV nutzen.

Die Freigabe dieses Dokuments erfolgt durch den Informationssicherheitsbeauftragten der KBV, die Inkraftsetzung durch den Vorstand der KBV. Dieses Dokument tritt nach Bekanntgabe in Kraft, gilt in der jeweils aktuellen veröffentlichten Form und ist verpflichtend anzuwenden.

1.3 ÄNDERUNGSDIENST

Die Verantwortung zur Pflege und Anpassung des vorliegenden Dokuments liegt beim Informationssicherheitsbeauftragten der KBV. Das geänderte Dokument wird komplett ausgetauscht. Die Änderungen sind in der Dokumentenhistorie aufgeführt. Der Revisionsstand wird jeweils um eins erhöht.

1.4 VERTEILER / VERTEILERDIENST

Für den Verteilungsdienst dieses Dokuments an die im Verteiler genannten Stellen ist der Informationssicherheitsbeauftragte der KBV zuständig. Die Empfänger entscheiden über die weitere Verteilung innerhalb ihrer Verantwortungsbereiche und stellen nachvollziehbar sicher, dass der letztgültige Stand dieses Dokuments den am Verfahren beteiligten Mitarbeitenden zur Verfügung steht. Diese Nachvollziehbarkeit wird als gegeben angenommen, wenn im Unternehmensportal und auf der Website der KBV die gültige Version des Dokumentes eingestellt ist.

Verteiler: Vorstand, Direktorat Verwaltung, Direktorat Personal, Stabsbereich Recht, Stabsbereich Strategie, Politik und Kommunikation, Dezernenten und Dezernentinnen, Leiter und Leiterinnen der selbständigen Organisationseinheiten, Unternehmensportal

1.5 KLASSIFIZIERUNG

Dieses Dokument ist öffentlich und unter www.kbv.de/iso27001.html für alle einsehbar.

2. REGELUNGEN

2.1 STELLENWERT DER INFORMATIONS- UND KOMMUNIKATIONSTECHNIK

Die KBV ist die politische Interessenvertretung der niedergelassenen Vertragsärzte und -psychotherapeuten. Sie vertritt die Belange ihrer Mitglieder bei Gesetzgebungsverfahren gegenüber der Bundesregierung. Zu den gesetzlichen Aufgaben der Körperschaft gehören des Weiteren die Wahrnehmung der Rechte der niedergelassenen Mediziner gegenüber den Krankenkassen sowie die Sicherstellung und die Gewährleistung der vertragsärztlichen und -psychotherapeutischen Versorgung. Als Einrichtung der ärztlichen Selbstverwaltung schließt die KBV Verträge mit dem GKV-Spitzenverband sowie anderen Sozialleistungsträgern ab. In diesen Vereinbarungen werden die Grundsätze der vertraglichen Beziehungen zwischen den oben genannten Partnern auf Landesebene festgelegt und Rahmenvorgaben für die Inhalte der Arznei- und Heilmittelvereinbarungen gemacht. Die KBV gestaltet mit den Krankenkassen die bundesweit geltende Gebührenordnung der niedergelassenen Ärzte, den einheitlichen Bewertungsmaßstab.

Die Informationsverarbeitung spielt eine Schlüsselrolle für die Erfüllung dieser Aufgaben. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informations- und Kommunikationstechnik maßgeblich unterstützt.

Definition der Bedeutung der Informationssicherheit für die KBV

Informationssicherheit bedeutet für uns, dass unsere Prozesse, deren Wirksamkeit wir kontinuierlich durch den Einsatz moderner Mittel der Informations- und Kommunikationstechnik weiterentwickeln, unter Minderung der unvermeidbaren Restrisiken, die Integrität der Daten gewährleisten, bei Bedarf verfügbar sind und zuverlässig funktionieren und den Schutz vertraulicher Informationen sicherstellen.

Im Mittelpunkt steht damit die Gewährleistung folgender Grundeigenschaften:

a) Verfügbarkeit,
   d. h. Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein
b) Integrität,
   d. h. Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten
c) Vertraulichkeit,
   d. h. Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden

Die Gewährleistung dieser Grundeigenschaften gilt als Maßgabe für alle Mitarbeitende der KBV, die an den im geltenden Anwendungsbereich [KBV_ISMS_RL_AWB] beschriebenen Prozessen beteiligt sind, unabhängig von ihrer Rolle und Stellung innerhalb der Gesamtorganisation sowie für alle externen Berater, Lieferanten und Servicepartner, die zu den im geltenden Anwendungsbereich beschriebenen Prozessen für die KBV Leistungen erbringen.

2.2 SICHERHEITSZIELE

Gemäß dem Leitbild der KBV, für ihre Mitglieder bessere Arbeitsbedingungen zu schaffen, nach größtmöglicher Zufriedenheit der Patienten zu streben und in der Bevölkerung und bei Partnern eine hohe Akzeptanz zu erzielen, verfolgt die KBV im Rahmen des Informationssicherheitsmanagements die folgenden Sicherheitsziele:

Sicherheitsziele der KBV

Informationen und Systeme werden bezüglich ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten toleriert werden können. Ausfallzeiten, die zu größeren Arbeitsverzögerungen oder Fristversäumnissen führen können, sollen durch entsprechende Maßnahmen vermieden werden.

Die Anforderungen an Integrität und Vertraulichkeit orientieren sich an der Gesetzeskonformität. Die Anforderungen des Datenschutzes sind bei der Bearbeitung personenbezogener Daten uneingeschränkt zu erfüllen.

ISMS-Maßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen verhindert werden.

Der Zugriff auf Informationen wird durch ein angemessenes Berechtigungskonzept begrenzt. Neben dem Schutz der IT-Infrastruktur - Netze, Server, Personalcomputer, Software - sind auch Gebäude und Räumlichkeiten angemessen zu schützen.

Das Bild der KBV in den Augen ihrer Mitglieder und Vertragspartner hängt entscheidend von der Zuverlässigkeit der Aufgabenerfüllung ab, weshalb größte Sorgfalt auf den bestimmungsgemäßen Gebrauch der Informationsverarbeitung zu verwenden ist, um einem Vertrauensverlust entgegen zu wirken.

2.3 STRATEGISCHE EINORDNUNG

Zur Erreichung der Sicherheitsziele und kontinuierlichen Verbesserung des Sicherheitsniveaus der KBV wird ein dokumentiertes Informationssicherheitsmanagementsystem (ISMS) festgelegt, umgesetzt, durchgeführt, überwacht, überprüft, instandgehalten und verbessert [KBV_ISMS_RL_ISM]. Grundlage des Informationssicherheitsmanagements der KBV sind die Maßgaben der ISO 27000 [DIN/ISO 27000:20014(E)] und der ISO 27001 [DIN ISO/IEC 27001:2015-03]. Zudem werden Empfehlungen der ISO 27002 [DIN ISO/IEC 27001:2013(E)] und darüber hinaus die des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie weiterer anerkannter Organisationen bei Bedarf genutzt.

Das ISMS bezieht sich dabei auf den nachfolgend definierten Anwendungsbereich:

Anwendungsbereich des ISMS

Der Anwendungsbereich des Informationssicherheitsmanagementsystems (ISMS) gilt für die Kassenärztliche Bundesvereinigung an allen Standorten, über das gesamte Spektrum der Produkte und Dienstleistungen sowie für alle Mitarbeitende und Prozesse des Unternehmens sowie beauftragter Unternehmen, einschließlich der erhobenen, verarbeiteten und genutzten Daten.

Basierend auf den Ergebnissen der Risikoanalyse können durch entsprechende ISMS-Maßnahmen Vorkehrungen getroffen werden, um Bußgelder, Strafen und Regressforderungen zu vermeiden sowie materiellen und immateriellen Schaden von der KBV abzuwenden und damit Risiken zu mindern [KBV_ISMS_RL_RSM].

ISMS-Maßnahmen werden nach Beschluss bzw. Freigabe unter Maßgabe der Einhaltung einschlägiger rechtlicher, vertraglicher und interner Regelungen realisiert. Ihrer Berücksichtigung wird hohe Priorität beigemessen. Bei Änderungen der Gesetzeslage werden die ISMS-Maßgaben zügig aktualisiert.

Durch geeignete Qualifizierungs- und Sensibilisierungsmaßnahmen zu Themen der Informationssicherheit sowie zu entsprechenden ISMS-Richtlinien, Verfahrensanweisungen und sonstigen Vorschriften wird das Sicherheitsbewusstsein der Mitarbeitende der KBV kontinuierlich aufrechterhalten und weiter entwickelt [KBV_ISMS_RL_HRM].

In der KBV ist ein gelenkter Prozess zur Sicherstellung des Geschäftsbetriebs (Business Continuity) aufrechtzuerhalten und weiter zu entwickeln, der die erforderlichen Informationssicherheitsanforderungen berücksichtigt [KBV_ISMS_RL_BCM].

Informationssicherheit ist eine ganzheitliche und strategische Aufgabe, die von allen Mitarbeitern ein verantwortungsbewusstes und engagiertes Handeln erfordert. Dies bezieht sich insbesondere auch auf die Meldung von und den Umgang mit Informationssicherheitsvorfällen. Mit der Organisation des ISMS erfolgt die Einbettung der verantwortlichen und unterstützenden Instanzen in die Aufbauorganisation der KBV [KBV_ISMS_RL_SIO].

Die Informationssicherheitspolitik wird durch weitere ISMS-Richtlinien (hierzu gehören insbesondere die in Kapitel 3.2 genannten) unterstützt und durch konkrete Dokumentierte Informationen und Prozessbeschreibungen operationalisiert. Alle ISMS-Dokumente unterliegen einer Lenkung [KBV_ISMS_RL_DKL].

Die Maßnahmen zur Erreichung der Sicherheitsziele umfassen dabei grundsätzlich die folgenden Bereiche:

- Informationssicherheitsrichtlinien (dieses Dokument)
  [DIN ISO/IEC 27001:2015-03, A.5]
- Organisation der Informationssicherheit
  [DIN ISO/IEC 27001:2015-03, A.6]
- Personalsicherheit
  [DIN ISO/IEC 27001:2015-03, A.7]
- Verwaltung der Werte
  [DIN ISO/IEC 27001:2015-03, A.8]
- Zugangssteuerung
  [DIN ISO/IEC 27001:2015-03, A.9]
- Kryptographie
  [DIN ISO/IEC 27001:2015-03, A.10]
- Physische und umgebungsbezogene Sicherheit
  [DIN ISO/IEC 27001:2015-03, A.11]

- Betriebssicherheit
  [DIN ISO/IEC 27001:2015-03, A.12]
- Kommunikationssicherheit
  [DIN ISO/IEC 27001:2015-03, A.13]
- Anschaffung, Entwicklung und Instandhalten von Systemen
  [DIN ISO/IEC 27001:2015-03, A.14]
- Lieferantenbeziehungen
  [DIN ISO/IEC 27001:2015-03, A.15]
- Handhabung von Informationssicherheitsvorfällen
  [DIN ISO/IEC 27001:2015-03, A.16]
- Informationssicherheitsaspekte beim Business Continuity Management
  [DIN ISO/IEC 27001:2015-03, A.17]
- Compliance
  [DIN ISO/IEC 27001:2015-03, A.18]

2.4 PERSÖNLICHE VERANTWORTUNG

Die Geschäftsprozesse und Unternehmenswerte der KBV können durch diverse Gefährdungen bedroht werden. Diese Gefährdungen gilt es zu identifizieren und hinsichtlich der daraus resultierenden Risiken zu bewerten.

Es ist die gemeinsame Pflicht von Führungskräften und Mitarbeitenden, ein dem Schutzbedarf angemessenes Sicherheitsniveau zu gewährleisten. Jeder einzelne Mitarbeitende, unabhängig von seiner Stellung in der Organisation und seinem Aufgabenbereich, trägt die Mitverantwortung für die Informationssicherheit in seinem Arbeitsumfeld. Es wird erwartet, dass jeder Mitarbeitende selbständig im Falle von erkannten Sicherheitsproblemen aktiv wird.

Zur Aufrechterhaltung und Weiterentwicklung des Sicherheitsbewusstseins und der entsprechenden Qualifikation sind daher bedarfsgerechte Schulungs- und Trainingsmaßnahmen für die Mitarbeitenden zu planen und umzusetzen [KBV_ISMS_RL_HRM]. Die Sensibilisierung ist eine Aufgabe des Informationssicherheitsbeauftragten [KBV_ISMS_RL_SIO].

Alle Mitarbeitenden sind verpflichtet, im Rahmen ihres Tätigkeitsbereichs Risiken zu identifizieren und weiterzugeben bzw. bei der angemessenen Risikobehandlung mitzuwirken und entsprechende Vorschläge zur Verbesserung zu unterbreiten. Ansprechpartner sind immer die unmittelbare Führungskraft und der Informationssicherheitsbeauftragte.

Die Richtlinie Informationssicherheit gibt an alle Mitarbeitende den eindeutigen Auftrag des Vorstandes, alle bestehenden und künftigen Vorgaben zur Erreichung der Sicherheitsziele zu beachten und umzusetzen.

2.5 MAßNAHMEN BEI VERSTÖßEN

Als Verstöße gegen die Maßgaben dieser und weiterer Richtlinien, Verfahrensanweisungen und sonstigen Vorschriften gelten alle Handlungen, die

a) die Sicherheit der Mitarbeitenden, Mitglieder, Vertragspartner oder der Einrichtungen und Systeme sowie der Informationen der KBV (Werte) beeinträchtigen
b) der KBV durch die Verletzung der Sicherheit tatsächlichen oder potenziellen materiellen oder immateriellen Schaden zufügen
c) den unberechtigten Zugriff auf Informationen, d. h. deren Preisgabe oder unautorisierte Änderung ermöglichen oder
d) die eine Kompromittierung des Rufes der KBV zur Folge haben.

Verstöße gegen Richtlinien, Verfahrensanweisungen und sonstige Vorschriften können zu erheblichen negativen Konsequenzen für die KBV führen. Deshalb ist bei vorsätzlichen und grob fahrlässigen Handlungen, die einen Verstoß darstellen, mit arbeitsrechtlichen Konsequenzen zu rechnen. Darüber hinaus können derartige Zuwiderhandlungen auch straf- oder zivilrechtliche Schritte nach sich ziehen. Die Grundlagen hierfür sind durch einen dokumentierten Disziplinarprozess festzuhalten [KBV_ISMS_DI_HRM].

3. VERWEISE UND BEGRIFFE

3.1 REFERENZIERTE MAßNAHMENZIELE UND MAßNAHMEN

REFERENZIERTE MAßNAHMEN UND MAßNAHMENZIELE		
Abschnitt/Control	Anforderung/Titel	Kapitel
Kap. 5.2.a (27001)	für den Zweck der Organisation angemessen ist	1.1
A.5.1 (27001)	Vorgaben der Leitung für Informationssicherheit	1.1
Kap. 5.1.1 (27002)	Informationssicherheitsleitlinien	1.1, 2.1, 2.2, 2.3, 2.5
Kap. 4.3 (27001)	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	2.3

3.2 REFERENZIERTE ISMS-DOKUMENTE

Die folgenden zitierten ISMS-Dokumente sind für die Anwendung dieses Dokumentes erforderlich. Bei datierten Verweisen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisen gilt die letzte Ausgabe des in Bezug genommen Dokuments.

REFERENZIERTE ISMS-DOKUMENTE	
[KBV_ISMS_RL_ISM]	Richtlinie Informationssicherheitsmanagement
[KBV_ISMS_RL_AWB]	Richtlinie Anwendungsbereich
[KBV_ISMS_RL_BCM]	Richtlinie Business Continuity Management
[KBV_ISMS_RL_DKL]	Richtlinie Lenkung von Dokumenten und Aufzeichnungen
[KBV_ISMS_RL_HRM]	Richtlinie Personalsicherheit
[KBV_ISMS_RL_RSM]	Richtlinie Risikomanagement
[KBV_ISMS_RL_SIO]	Richtlinie Sicherheitsorganisation
[KBV_ISMS_DI_HRM]	Dokumentierte Information Disziplinarkonzept

3.3 NORMATIVE VERWEISE

Die folgenden zitierten normativen Grundlagen sind für die Anwendung dieses Dokumentes erforderlich. Bei datierten Verweisen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisen gilt die letzte Ausgabe der in Bezug genommen normativen Grundlage.

NORMATIVE VERWEISE	
[DIN ISO/IEC 27000:2014(E)]	Information technology – Security techniques – Information security techniques – Information security management systems – Overview and vocabulary
[DIN ISO/IEC 27001:2015-03]	Informationstechnik – IT-Sicherheitsverfahren Informationssicherheits-Managementsysteme – Anforderungen
[DIN ISO/IEC 27002:2013(E)]	Information technology – Security techniques – Code of practice for information security controls

3.4 BEGRIFFE

3.4.1 Anwendungsbereich

Grenzen und Anwendbarkeit des Informationssicherheitsmanagementsystems (ISMS), unter Berücksichtigung von externen und internen Themen der Organisation, von Anforderungen interessierter Parteien sowie von Schnittstellen zu anderen Organisationen mit Bezug zur Informationssicherheit.

[DIN ISO/IEC 27001:2015-03]

3.4.2 Daten-/Informations-/Werteverantwortung

Die Datenverantwortung im Sinne des Datenschutzgesetzes hat die verarbeitende Stelle. Innerhalb dieser Stelle müssen Daten-/Informationsverantwortliche bestimmt werden. Grundsätzlich sind dies die für den im Anwendungsbereich definierten KBV Geschäftsprozess verantwortliche Mitarbeitende. Diese sind innerhalb der Risikoanalyse als Werteverantwortliche definiert. Diese befinden u. a. über die Klassifizierung der Daten in Bezug auf die Vertraulichkeitsanforderungen und machen Vorgaben für die Vergabe von Zugriffsrechten. Die Datenverantwortung ist schriftlich zu dokumentieren.

3.4.3 Informationssicherheit

Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden.

[DIN ISO/IEC 27000:2014(E)]

3.4.4 Informationssicherheitsmanagementsystem (ISMS)

Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.

[DIN ISO/IEC 27000:2014(E)]

3.4.5 Integrität

Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten.

[DIN ISO/IEC 27000:2014(E)]

3.4.6 Mitarbeitende

Mitarbeitende wird als Oberbegriff für alle Angestellten, Auftragnehmer und Dritte gemäß den nachfolgenden Definitionen verwendet.

- **Angestellte**

  Unter Angestellten werden alle Beschäftigten verstanden, die einer nichtselbständigen Tätigkeit nachgehen.

- **Auftragnehmer**

  Auftragnehmer sind durch Vertrag (zum Beispiel Werkvertrag oder Dienstvertrag) Beauftragte, die nicht Angestellte sind.

- **Dritte**

  Dritte sind Personen, die weder Angestellte noch Auftragnehmer sind, jedoch Einrichtungen und Informationen der Organisation nutzen.

3.4.7 Verfügbarkeit

Eigenschaft von Werten, auf Verlangen zugänglich und nutzbar zu sein.

[DIN ISO/IEC 27000:2014(E)]

3.4.8 Vertraulichkeit

Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden.

[DIN ISO/IEC 27000:2014(E)]

3.4.9 Wert

Werte sind alle Informationen und Geschäftsprozesse (primäre Werte) sowie Hardware, Software, Netzwerk, Personal, Standorte und die Organisation (unterstützende Werte), die einen Schutzbedarf bezogen auf ihre Verfügbarkeit, Vertraulichkeit bzw. Integrität haben.

3.4.10 Zutritt

Betreten von Bereichen und Räumen, in denen informationsverarbeitende Einrichtungen aufgestellt bzw. Informationen verwahrt werden.

3.4.11 Zugang

Möglichkeit der Nutzung von informationsverarbeitenden Einrichtungen (zum Beispiel Systemzugang via Login).

3.4.12 Zugriff

Ausüben von Rechten auf Informationen durch Personen (zum Beispiel Zugriff auf Dateien gemäß Benutzerrollen und -berechtigungen).

4. INKRAFTSETZUNG

Berlin, den

Dr. Andreas Gassen	Dr. Stephan Hofmeister	Dr. Thomas Kriedel
Vorstandsvorsitzender	Stellvertretender Vorstandsvorsitzender	Mitglied des Vorstands