Karlsruher Institut für Technologie

IT-Sicherheitskonzept für das KIT

Regelung zur Umsetzung von IT-Sicherheitsmaßnahmen

Andreas Lorenz · Tobias Dussa

DER IT-SICHERHEITSBEAUFTRAGTE

Kontakt

Karlsruhe Institute of Technology (KIT)

Andreas Lorenz
IT-Sicherheitsbeauftragter

Campus Nord
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen

Telefon: 0721 608-24500
Fax: 0721 608-24972
E-Mail: andreas.lorenz@kit.edu

Tobias Dussa
Stellvertretender IT-Sicherheitsbeauftragter

Campus Süd
Zirkel 2
76131 Karlsruhe

Telefon: 0721 608-42479
Fax: 0721 608-9-42479
E-Mail: tobias.dussa@kit.edu

www.itsb.kit.edu

Herausgeber

Karlsruhe Institute of Technology (KIT)
Steinbuch Centre for Computing (SCC)

Zirkel 2 | 76131 Karlsruhe

E-Mail: itsb@kit.edu

Stand 2018-03-22 (Revision 12)

www.kit.edu

Inhaltsverzeichnis

Versionshistorie

Version	Inkrafttreten	Autor(en)	Änderung(en)
1	2015-03-17	Lorenz, Andreas; Dussa, Tobias	Initiale Revision.
2	2018-03-22	Lorenz, Andreas; Dussa, Tobias	Referenzen auf ISO-Controls und BSI-Maßnahmen aktualisiert; Abschnitt eingefügt (3.7); Abschnitte umbenannt (2.2, 2.6); Abschnitte aktualisiert (2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 3.1, 3.2, 3.3, 3.4, 3.6, 3.10, 3.11, 3.12, 3.13, 3.14, 3.15).

1 Einleitung/Präambel

1.1 Das IT-Sicherheitskonzept

Das IT-Sicherheitskonzept des KIT dient der Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten IT-Sicherheitsziele zu erreichen. Gemäß des im Dezember 2017 verabschiedeten IV-Governance-Frameworks am KIT, das unter https://www.kit.edu/downloads/cio/IV-Gov-Framework.pdf verfügbar ist, ist eine Perspektiverweiterung hin zur Informationssicherheit angedacht. Bis ein Informationssicherheitskonzept ausgearbeitet und beschlossen ist, gilt das vorliegende Konzept. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess des KIT. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Aus diesem Grund muss das IT-Sicherheitskonzept sorgfältig geplant und umgesetzt sowie regelmäßig überprüft werden; diese Revision findet jährlich statt.

Nicht alle IT-Verbünde des KIT müssen durch ein einziges IT-Sicherheitskonzept abgedeckt werden. Es kann weitere IT-Sicherheitskonzepte geben, die verschiedene Informationsverbünde des KIT abdecken. Ebenso können komplexe Geschäftsprozesse oder Anwendungen in eigenen IT-Sicherheitskonzepten behandelt werden. Dies empfiehlt sich vor allem bei der Einführung neuer Aufgaben oder Anwendungen im KIT.

Der Geltungsbereich des IT-Sicherheitskonzepts umfasst immer einen Informationsverbund und stellt detailliert den Teil dar, für den das IT-Sicherheitskonzept umgesetzt werden muss. Ein Informationsverbund kann sich somit auf Fachaufgaben, Geschäftsprozesse oder Organisationseinheiten beziehen. Er umfasst alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in diesem Anwendungsbereich der Informationsverarbeitung dienen. Der Informationsverbund muss so festgelegt sein, dass die betrachteten Geschäftsprozesse und Informationen dieser Informationsverbund vollständig zugeordnet werden können. Die Abhängigkeiten aller sicherheitsrelevanten Prozesse sind zu berücksichtigen. Die Schnittstellen zu den anderen Verbünden müssen klar definiert werden, so dass der Informationsverbund in der Gesamtorganisation eine sinnvolle Mindestgröße einnimmt.

1.2 Aufbau und Vorgehensweise

Das IT-Sicherheitskonzept des KIT ist thematisch in zwei Teile gegliedert. Der erste Teil behandelt die Organisation des IT-Sicherheitsmanagements, der zweite Teil beleuchtet die technischen Maßnahmen für die Umsetzung der IT-Sicherheitsarchitektur.

Die Grundlage für dieses IT-Sicherheitskonzept bilden zum einen das Grundschutzhandbuch des Bundesamtes für IT-Sicherheit in der Informationstechnik (BSI) und zum anderen der ISO-Standard 27001 (Information Security Management Systems). Die beschriebenen Maßnahmen sind nach diesen beiden Standards ausgerichtet. Die Orientierung des Konzepts an nationalen und internationalen Standards bildet eine solide Basis für die zukünftige Weiterentwicklung der IT-Sicherheit am KIT auf organisatorischer und technischer Ebene. Diese Ausrichtung unterstützt eine mögliche spätere Zertifizierung nach den entsprechenden Standards.

Auf weitergehende Information zu aufgeführten Maßnahmen wird gegebenenfalls in den Textpassagen verwiesen, es werden die entsprechenden Dokumente und Quellen benannt. Da die dokumentierten Maßnahmen auf Bausteine der Grundschutzkataloge des BSI beziehungsweise auf Control Objects der ISO 27001 abgebildet werden können, sind diese Referenzen in den einzelnen Bausteinen aufgelistet.

Die beschriebenen Maßnahmen können nur wirksamen Schutz für das KIT bieten, wenn diese innerhalb jeder Organisationseinheit beziehungsweise jedes Informationsverbunds des KIT konsequent umgesetzt werden.

Karlsruhe, den 22. März 2018

Die IT-Sicherheitsbeauftragten des Karlsruher Instituts für Technologie
Andreas Lorenz und Tobias Dussa

2 Organisation des IT-Sicherheitsmanagements

Die Bedeutung der Informationsverarbeitung und -versorgung für das KIT als Institution, für alle am KIT tätigen Personengruppen sowie für die zugrundeliegenden Geschäftsprozesse des KIT in Forschung, Lehre und Innovation verlangt einen sicheren und rechtskonformen Betrieb der IT wie auch einen entsprechenden Umgang mit Information.

Die IT-Sicherheit bildet die Voraussetzung für einen verlässlichen IT-Betrieb, beispielsweise müssen sowohl Datenspionage als auch Rechnerinfektion durch Schadsoftware erfolgreich abgewehrt werden. Ebenso müssen die Nachvollziehbarkeit und die Integrität von IT-gestützten Prozessen gewährleistet sein.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert zur Erreichung dieser und weiterer Ziele im Kontext der IT-Sicherheit konkrete Vorgehensweisen auf Basis von Gefährdungs- und Maßnahmenkatalogen. Zum Aufbau einer geeigneten Organisationsstruktur wird die Definition der Funktionen eines IT-Sicherheitsbeauftragten und eines IT-Sicherheitsmanagement-Teams empfohlen. Das IT-Sicherheitsmanagement orientiert sich dabei an dem "Plan,-Do,-Check,-Act"-Paradigma (PDCA). Diese Vorgehensweise erlaubt die iterative Einführung eines Managementsystems mit der Möglichkeit einer schrittweisen Verbesserung der Prozesse.

Begrifflichkeiten

Im folgenden werden einige in diesem Dokument verwendete Begriffe erläutert. Die Definitionen lehnen sich an den BSI-Standard 100-2 an.

IT-Sicherheitsprozess: Um ein angemessenes IT-Sicherheitsniveau erreichen und aufrecht erhalten zu können, ist es notwendig, einen kontinuierlichen IT-Sicherheitsprozess zu etablieren und eine angemessene Strategie für Informationssicherheit (IT-Sicherheitsstrategie) festzulegen. Die IT-Sicherheitsstrategie dient der Planung des weiteren Vorgehens, um die gesetzten Sicherheitsziele zu erreichen (siehe unten).

IT-Sicherheitsstrategie: Die IT-Sicherheitsstrategie dient der Planung des weiteren Vorgehens, um die gesetzten Sicherheitsziele zu erreichen. Sie wird vom Management vorgegeben und basiert auf den Geschäftszielen eines Unternehmens beziehungsweise dem Auftrag einer Behörde. Das Management gibt grundlegende Sicherheitsziele vor und legt fest, welches IT-Sicherheitsniveau im Hinblick auf die Geschäftsziele und Fachaufgaben angemessen ist.

IT-Sicherheitsziele: Aus den grundsätzlichen Zielen der Institution und den allgemeinen Rahmenbedingungen werden allgemeine IT-Sicherheitsziele abgeleitet. Aus diesen werden später konkrete Sicherheitsanforderungen an den Umgang mit Informationen und den IT-Betrieb abgeleitet.

IT-Sicherheitsleitlinie: Die IT-Sicherheitsleitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution. In ihr wird beschrieben, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll. Sie beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch über die Sicherheitsziele das angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

IT-Sicherheitskonzept: Ein IT-Sicherheitskonzept dient zur Umsetzung der IT-Sicherheitsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten IT-Sicherheitsziele einer Institution zu erreichen. Das IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens beziehungsweise einer Behörde. Jede konkrete IT-Sicherheitsmaßnahme muss sich letztlich darauf zurückführen lassen.

IT-Sicherheitsrichtlinie: Als IT-Sicherheitsrichtlinien werden Regelungen und Vorgaben bezeichnet, die die übergreifenden Belange der Informationssicherheit regeln.

IT-Sicherheitsmaßnahme: Als IT-Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die dazu dienen, IT-Sicherheitsrisiken zu steuern und diesen entgegenzuwirken. Dies schließt sowohl organisatorische als auch personelle, technische oder infrastrukturelle IT-Sicherheitsmaßnahmen ein.

2.1 IT-Sicherheitsbeauftragter des KIT

Für die operative Seite des IT-Sicherheitsmanagements ist folgende Funktion des IT-Sicherheitsbeauftragten des KIT (ITSB) geschaffen. Zu den Aufgaben des IT-Sicherheitsbeauftragten des KIT gehört, wie in den Grundschutzkatalogen des BSI vorgeschlagen, unter anderem

- den IT-Sicherheitsprozess zu steuern und zu koordinieren,
- den IV-Bevollmächtigten (IV-B; siehe auch Abschnitt 2.5) bei der Erstellung der IT-Sicherheitsleitlinie zu unterstützen,
- die Erstellung von IT-Sicherheitsrichtlinien zu initiieren und zu koordinieren,
- die Erstellung des IT-Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte zu koordinieren,
- den Realisierungsplan für die IT-Sicherheitsmaßnahmen zu erstellen und deren Realisierung zu initiieren und zu überprüfen,
- der Leitungsebene und dem IT-Sicherheitsmanagement-Team zu berichten,
- sicherheitsrelevante Projekte zu koordinieren und den Informationsfluss zwischen IT-Beauftragten der Organisationseinheiten, IT-Projekt-Beauftragten sowie IT-System-Sicherheitsbeauftragten sicherzustellen,
- sicherheitsrelevante Zwischenfälle zu untersuchen, sowie
- Sensibilisierungs- und Schulungsmaßnahmen zu IT-Sicherheit zu initiieren und zu steuern.

Diese Aufgaben sind so umfangreich, dass diese durch das IT-Sicherheitsmanagement-Team unterstützt werden müssen.

2.1.1 Beteiligte

Federführung: KIT-Präsidium

2.1.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- **M 2.195:** »Erstellung eines Sicherheitskonzepts«
- **M 2.199:** »Aufrechterhaltung der Informationssicherheit«
- **M 2.200:** »Management-Berichte zur Informationssicherheit«
- **M 2.201:** »Dokumentation des Sicherheitsprozesses«
- **M 2.335:** »Festlegung der Sicherheitsziele und -strategie«
- **M 2.338:** »Erstellung von zielgruppengerechten Sicherheitsrichtlinien«
- **M 2.339:** »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.5.1.1: "Information security policy document"
- A.5.1.2: "Review of the information security policy"
- A.6.1.1: "Management commitment to information security"
- A.6.1.2: "Information security coordination"
- A.6.1.3: "Allocation of information security responsibilities"
- A.10.8.5: "Business information systems"

2.2 IT-Sicherheitsteam des KIT

Das IT-Sicherheitsteam unterstützt den ITSB auf der operativen Ebene. Neben der Realisierung der notwendigen Maßnahmen bildet es als Computernotfallteam (KIT-CERT) die zentrale Koordinationsstelle des KIT bei Missbrauch von IT-Diensten oder -Anlagen. Es ist als Teil des zentralen IT-Dienstleisters Steinbuch Centre for Computing (SCC) nah an den wesentlichen zentralen technischen Systemen und hat direkten Kontakt zu den verantwortlichen Mitarbeitern, um eine zügige Bearbeitung von Vorfällen zu gewährleisten.

2.2.1 Beteiligte

Federführung: SCC

2.2.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- **M 2.195:** »Erstellung eines Sicherheitskonzepts«
- **M 2.199:** »Aufrechterhaltung der Informationssicherheit«
- **M 2.201:** »Dokumentation des Sicherheitsprozesses«
- **M 2.338:** »Erstellung von zielgruppengerechten Sicherheitsrichtlinien«
- **M 2.339:** »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.5.1.1:** "Information security policy document"
- **A.5.1.2:** "Review of the information security policy"
- **A.6.1.1:** "Management commitment to information security"
- **A.6.1.2:** "Information security coordination"
- **A.6.1.3:** "Allocation of information security responsibilities"
- **A.10.8.5:** "Business information systems"

2.3 IT-Sicherheitsleitlinie, Ziele und Strategie

Die IT-Sicherheitsleitlinie dokumentiert die Richtlinie, nach welchen Grundsätzen das Thema IT-Sicherheit im KIT behandelt wird. Die Leitaussagen zur IT-Sicherheitsstrategie werden in einer IT-Sicherheitsleitlinie zusammengefasst, um die zu verfolgenden IT-Sicherheitsziele und das angestrebte IT-Sicherheitsniveau zu dokumentieren.

2.3.1 IT-Sicherheitsleitlinie des Karlsruher Instituts für Technologie (KIT)

Die IT-Sicherheitsleitlinie ist durch Beschluss des Präsidiums des KIT am 1. Oktober 2009 in Kraft getreten. Sie dokumentiert die Ziele des IT-Sicherheitsmanagements und benennt unter anderen die mit diesem Thema betrauten Parteien. Die IT-Sicherheitsleitlinie ist unter dem URL http://www.kit.edu/downloads/KIT-Sicherheitsleitlinie.pdf zu finden.

Sie folgt dem Grundsatz, dass der Aufwand für die Schutzmaßnahmen stets in Relation zum erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen ist, weil sich nur so auf Dauer das Bedürfnis nach Sicherheit und die Freiheit der Forschung und Lehre miteinander vereinbaren lassen.

Gemäß IT-Sicherheitsleitlinie schützt das KIT seine Interessen und sein Ansehen in der Öffentlichkeit durch die Sicherung seiner Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit. Zu den IT-Sicherheitszielen des KIT zählen

- die Gewährleistung der Verfügbarkeit der IT-Systeme, Programme und Daten, der Schutz der Integrität der IT-Systeme, Programme und Daten;
- die Verhinderung des Missbrauchs der IT-Systeme, Programme und Daten (zweckwidrige Nutzung, Nutzung durch Unbefugte), sowohl aus Gründen des Selbstschutzes als auch zum Schutz Dritter;
- die Handhabung der vertraulichen Informationen unabhängig von der Art ihrer Aufzeichnung derart, dass ihre Vertraulichkeit jederzeit sichergestellt ist;
- die Sicherstellung der Integrität, Funktionsfähigkeit und Vertraulichkeit von Arbeitsergebnissen und von Projektdaten;
- die Einhaltung der einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen; sowie
- die Wahrung der Persönlichkeitsrechte der Mitglieder und der Angehörigen.

2.3.2 Beteiligte

Federführung: KIT-Präsidium

2.3.3 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.192:** »Erstellung einer Leitlinie zur Informationssicherheit«
- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«

- M 2.195: »Erstellung eines Sicherheitskonzepts«
- M 2.335: »Festlegung der Sicherheitsziele und -strategie«
- M 2.336: »Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene«
- M 2.339: »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.5.1.1: "Information security policy document"
- A.6.1.1: "Management commitment to information security"
- A.6.1.2: "Information security coordination"
- A.6.1.3: "Allocation of information security responsibilities"

2.4 IT-Sicherheitsrichtlinien

Die IT-Sicherheitsrichtlinien bilden das Regelwerk für die Implementierung einer IT-Sicherheitsarchitektur. Sie werden anhand der im IT-Sicherheitskonzept definierten Sicherheitsstandards formuliert und realisiert. Der ITSB führt die Liste der IT-Sicherheitsrichtlinien und stellt sie auf seiner Webseite zur Verfügung. Diese Webseite ist erreichbar unter dem URL https://www.itsb.kit.edu/.

2.4.1 Beteiligte

Federführung: ITSB

2.4.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.338:** »Erstellung von zielgruppengerechten Sicherheitsrichtlinien«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.10.8.5:** "Business information systems"

2.5 Organisatorische Verantwortung

Die Initiative zum Informationssicherheitsmanagement geht vom Präsidium des KIT aus. Es trägt die Verantwortung dafür, dass in der Institution gesetzliche Anforderungen und Geschäftsbedingungen eingehalten sowie interne Regelungen beachtet werden.

Die einzelnen Strukturen und Gremien sind in der Leitlinie zur IT-Sicherheit am KIT ausgeführt, die unter dem folgenden URL verfügbar ist: https://www.itsb.kit.edu/p/it-sicherheitsleitlinie.

2.5.1 Beteiligte

Federführung: KIT-Präsidium

2.5.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.192:** »Erstellung einer Leitlinie zur Informationssicherheit«
- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- **M 2.200:** »Management-Berichte zur Informationssicherheit«
- **M 2.201:** »Dokumentation des Sicherheitsprozesses«
- **M 2.335:** »Festlegung der Sicherheitsziele und -strategie«
- **M 2.336:** »Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene«
- **M 2.339:** »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.5.1.1:** "Information security policy document"
- **A.5.1.2:** "Review of the information security policy"
- **A.6.1.1:** "Management commitment to information security"
- **A.6.1.2:** "Information security coordination"
- **A.6.1.3:** "Allocation of information security responsibilities"

2.6 IT-Sicherheit am Steinbuch Centre for Computing

Das Steinbuch Centre for Computing unterhält als zentrale Koordinierungsstelle für das Themengebiet IT-Sicherheit die Abteilung IT-Sicherheit und Service-Management (ISM). ISM erarbeitet sowohl innerhalb des SCC wie auch darüber hinaus technische Lösungen, die auch den Vorgaben des Datenschutzes sowie der gesetzlichen Sachlage entsprechen. Außerdem organisiert ISM innerhalb des SCC regelmäßige Treffen, um laufende Projekte zu koordinieren und neue Anforderungen an bestehende Lösungen mit den anderen Abteilungen zu erörtern.

Zudem ist das KIT-CERT in der Abteilung ISM und damit im SCC verankert.

2.6.1 Beteiligte

Federführung: SCC

2.6.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- **M 2.195:** »Erstellung eines Sicherheitskonzepts«
- **M 2.199:** »Aufrechterhaltung der Informationssicherheit«
- **M 2.339:** »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.5.1.1:** "Information security policy document"
- **A.5.1.2:** "Review of the information security policy"
- **A.6.1.2:** "Information security coordination"
- **A.6.1.3:** "Allocation of information security responsibilities"

2.7 IT-Beauftragte im KIT

Der zentrale IT-Dienstleister SCC stellt in der Regel einen Teil eines IT-Dienstes bereit, der bei einer Organisationseinheit genutzt wird. Ein weiterer Teil wird oftmals in der OE selbst erbracht, zugeschnitten auf deren spezifischen Bedarf. In diesen Fällen teilen sich das SCC und die OE die Verantwortung des ordnungsgemäßen Betriebs des entsprechenden IT-Dienstes. Für die partnerschaftliche Zusammenarbeit in IT-Belangen, insbesondere von der OE und dem SCC, sind aus der OE sogenannte IT-Beauftragte zu benennen. Die IT-Beauftragten und die Nutzer setzen die Richtlinien des KIT in den Organisationseinheiten um. Die IT-Beauftragten sind dort Ansprechpartner für alle IT-relevanten Aspekte.

2.7.1 Beteiligte

Federführung:	SCC
Zusätzlich beteiligt:	Leitung und ITB der OE

2.7.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.193: »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- M 2.195: »Erstellung eines Sicherheitskonzepts«
- M 2.199: »Aufrechterhaltung der Informationssicherheit«
- M 2.339: »Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.5.1.1: "Information security policy document"
- A.5.1.2: "Review of the information security policy"
- A.6.1.2: "Information security coordination"
- A.6.1.3: "Allocation of information security responsibilities"

2.8 Kontinuierliche IT-Sicherheitsprozesse

Die Gewährleistung von Informationssicherheit ist strategische Aufgabe des IT-Sicherheitsmanagements, das Ziele festlegt, effiziente Organisationsstrukturen aufbaut, Prozesse entwickelt und angemessene Schutzmaßnahmen umsetzt. Die getroffenen Entscheidungen werden kontinuierlich überprüft und bei Bedarf an geänderte Bedingungen angepasst. Veränderungen der inneren Strukturen einer Institution (Geschäftsprozesse, Fachaufgaben, organisatorische Gliederung) werden ebenso berücksichtigt wie solche in den äußeren Rahmenbedingungen (Gesetze, Verordnungen, Verträge), neuartige Bedrohungsszenarien ebenso wie Weiterentwicklungen der Sicherheitstechnik.

2.8.1 Beteiligte

Federführung: ITSB

2.8.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.193:** »Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit«
- **M 2.195:** »Erstellung eines Sicherheitskonzepts«
- **M 2.199:** »Aufrechterhaltung der Informationssicherheit«
- **M 2.200:** »Management-Berichte zur Informationssicherheit«
- **M 2.335:** »Festlegung der Sicherheitsziele und -strategie«
- **M 2.338:** »Erstellung von zielgruppengerechten Sicherheitsrichtlinien«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.5.1.1:** "Information security policy document"
- **A.5.1.2:** "Review of the information security policy"
- **A.6.1.1:** "Management commitment to information security"
- **A.6.1.2:** "Information security coordination"
- **A.6.1.3:** "Allocation of information security responsibilities"
- **A.10.8.5:** "Business information systems"

3 Technische Maßnahmen für die Umsetzung der IT-Sicherheitsarchitektur

3.1 Änderungsmanagement

Das Änderungsmanagement (auch Changemanagement) dokumentiert alle system- und sicherheitsrelevanten Arbeiten an den Systemen des KIT. Dabei können in einer Datenbank des Änderungsmanagements sämtliche IT-Ressourcen erfasst werden, so dass ein konsistenter Blick auf die IT-Landschaft des KIT möglich ist.

3.1.1 Beteiligte

Federführung:	Betreiber von IT-Diensten
Zusätzlich beteiligt:	ITB

3.1.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.221: »Änderungsmanagement«
- M 2.421: »Planung des Patch- und Änderungsmanagementprozesses«
- M 2.422: »Umgang mit Änderungsanforderungen«
- M 2.423: »Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement«
- M 2.424: »Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen«
- M 2.425: »Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement«
- M 2.426: »Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse«
- M 4.324: »Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.1.1: "Documentation of operating procedures"
- A.10.1.2: "Change Management"

3.2 Behandlung von Sicherheitsvorfällen – KIT-CERT

Das KIT-CERT wird durch die Abteilung IT-Sicherheit und Service-Management (ISM) des Steinbuch Centre for Computing (SCC) betrieben. Das KIT-CERT stellt den zentralen Ansprechpartner für die Themen IT-Sicherheit und Computermissbrauch dar und stellt in den folgenden Themengebieten Dienstleistungen für das KIT bereit.

3.2.1 Reaktive Dienste

- Koordination von Aktivitäten bei sicherheitsrelevanten Vorfällen oder Vorfällen im Zusammenhang mit Computermissbrauch,
- Incident response bei unmittelbaren Sicherheitsvorfällen sowie
- computerforensische Untersuchungen.

Im Rahmen der Behandlung von IT-Sicherheitsvorfällen kann das KIT-CERT Datenträger und Systeme zum Zweck der forensischen Untersuchung sicherstellen. Durch die forensische Untersuchung soll es ermöglicht werden, Angriffe auf die IuK-Infrastruktur des KIT zu analysieren, daraus entstehenden Gefahren adäquat zu begegnen und Schaden vom KIT abzuwenden.

3.2.2 Proaktive Dienste

- Betrieb von Netzsicherheitssystemen in verschiedenen Schichten sowie
- Überwachung des Verkehrsdatenstroms auf schadhafte Aktivität.

3.2.3 Beratungsdienste

- Beratung zum Thema Informations- und Computersicherheit,
- Veröffentlichung von Gutachten zu für das KIT relevanten Fragestellungen sowie
- Mitarbeit bei der Erstellung und Veröffentlichung von IT-Sicherheitsrichtlinien.

3.2.4 Weitere Dienste

Darüber hinaus arbeitet das KIT-CERT bei Anfragen von Sicherheitsbehörden eng mit der Dienstleistungseinheit Rechtsangelegenheiten (RECHT) des KIT zusammen. Das KIT-CERT koordiniert in diesen Fällen auch die Bearbeitung der Vorfälle.

Weitere Informationen zu dieser Dienstleistung des SCC sind unter dem URL https://cert.kit.edu zu finden.

3.2.5 Beteiligte

Federführung:	KIT-CERT
Zusätzlich beteiligt:	SCC

3.2.6 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 6.58: »Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen«
- M 6.59: »Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen«
- M 6.60: »Festlegung von Meldewegen für Sicherheitsvorfälle«
- M 6.61: »Eskalationsstrategie für Sicherheitsvorfälle«
- M 6.62: »Festlegung von Prioritäten für die Behandlung von Sicherheitsvorfällen«
- M 6.64: »Behebung von Sicherheitsvorfällen«
- M 6.65: »Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen«
- M 6.66: »Nachbereitung von Sicherheitsvorfällen«
- M 6.67: »Einsatz von Detektionsmaßnahmen für Sicherheitsvorfälle«
- M 6.68: »Effizienzprüfung des Managementsystems zur Behandlung von Sicherheitsvorfällen«
- M 6.121: »Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen«
- M 6.122: »Definition eines Sicherheitsvorfalls«
- M 6.123: »Einrichtung eines Expertenteams für die Behandlung von Sicherheitsvorfällen«
- M 6.124: »Festlegung der Schnittstellen der Sicherheitsvorfallbehandlung zur Störungs- und Fehlerbehebung«
- M 6.125: »Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen«
- M 6.126: »Einführung in die Computer-Forensik«
- M 6.127: »Etablierung von Beweissicherungsmaßnahmen bei Sicherheitsvorfällen«
- M 6.128: »Schulung an Beweismittelsicherungswerkzeugen«
- M 6.130: »Erkennen und Erfassen von Sicherheitsvorfällen«
- M 6.131: »Qualifizieren und Bewerten von Sicherheitsvorfällen«
- M 6.132: »Eindämmen der Auswirkung von Sicherheitsvorfällen«
- M 6.133: »Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen«
- M 6.134: »Dokumentation von Sicherheitsvorfällen«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.10.1: “Audit logging”
- A.10.10.2: “Monitoring system in use”
- A.10.10.3: “Protection of log information”
- A.10.10.4: “Administrator and operator logs”
- A.10.10.5: “Fault logging”

3.3 Datensicherung und Datenarchivierung

Die Verantwortung für die Datensicherung liegt sowohl beim Benutzer selbst als auch beim IT-Betreiber. Aus dem Schutzbedarf der zu sichernden Daten ergeben sich Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit. Bei der Datensicherung muss sichergestellt sein, dass diese Anforderungen erfüllt werden.

Darüber hinaus werden die Entscheidungsträger benannt, die eine Daten-Restaurierung veranlassen können. Geklärt wird weiterhin, wer berechtigt ist, auf Datensicherungsträger zuzugreifen, insbesondere wenn sie in Datensicherungsarchiven ausgelagert sind. Es wird sichergestellt, dass nur Berechtigte Zutritt erhalten. Abschließend wird definiert, wer berechtigt ist, eine Daten-Restaurierung des Gesamtdatenbestandes oder ausgewählter, einzelner Dateien operativ durchzuführen.

Bei der Festlegung der Verantwortlichkeit wird insbesondere der Vertraulichkeits-, Integritätsbedarf der Daten und die Vertrauenswürdigkeit der zuständigen Mitarbeiter betrachtet. Es wird sichergestellt, dass der Verantwortliche erreichbar und ein Vertreter benannt und eingearbeitet ist. Die Kenntnisse und datenverarbeitungsspezifischen Fähigkeiten der IT-Benutzer entscheiden darüber, ob die Datensicherung eigenverantwortlich je IT-Benutzer oder anderweitig durchgeführt wird. Sind die Kenntnisse der IT-Benutzer nicht ausreichend, ist die Verantwortung dem Systemadministrator oder einer speziell ausgebildeten Person zu übertragen.

3.3.1 Beteiligte

Federführung:	SCC
Zusätzlich beteiligt:	ITB

3.3.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 1.59: »Geeignete Aufstellung von Speicher- und Archivsystemen«
- M 1.60: »Geeignete Lagerung von Archivmedien«
- M 2.137: »Beschaffung eines geeigneten Datensicherungssystems«
- M 2.242: »Zielsetzung der elektronischen Archivierung«
- M 2.243: »Entwicklung des Archivierungskonzepts«
- M 2.244: »Ermittlung der technischen Einflussfaktoren für die elektronische Archivierung«
- M 2.257: »Überwachung der Speicherressourcen von Archivmedien«
- M 2.262: »Regelung der Nutzung von Archivsystemen«
- M 2.263: »Regelmäßige Aufbereitung von archivierten Datenbeständen«
- M 2.266: »Regelmäßige Erneuerung technischer Archivsystem-Komponenten«
- M 3.34: »Einweisung in die Administration des Archivsystems«
- M 3.35: »Einweisung der Benutzer in die Bedienung des Archivsystems«
- M 4.168: »Auswahl eines geeigneten Archivsystems«
- M 4.169: »Verwendung geeigneter Archivmedien«
- M 4.172: »Protokollierung der Archivzugriffe«
- M 6.20: »Geeignete Aufbewahrung der Backup-Datenträger«

- M 6.21: »Sicherungskopie der eingesetzten Software«
- M 6.22: »Sporadische Überprüfung auf Wiederherstellbarkeit von Datensicherungen«
- M 6.32: »Regelmäßige Datensicherung«
- M 6.33: »Entwicklung eines Datensicherungskonzepts«
- M 6.34: »Erhebung der Einflussfaktoren der Datensicherung«
- M 6.35: »Festlegung der Verfahrensweise für die Datensicherung«
- M 6.36: »Festlegung des Minimaldatensicherungskonzeptes«
- M 6.37: »Dokumentation der Datensicherung«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.5.1: "Information back-up"

3.4 IT-Sicherheitssensibilisierung und -schulung

IT-Sicherheitssensibilisierungen für Nutzer der Informations- und Kommunikationstechnik sind notwendig, um zu verstehen, dass die Sicherheit von Rechnersystemen auch zu großen Teilen vom Benutzerverhalten selbst abhängt. Um dieses Bewusstsein zu schaffen, müssen entsprechende Informationen an die Nutzerschaft herausgegeben oder diese in Informationsveranstaltungen auf diesen Sachverhalt hingewiesen werden. Das SCC bietet entsprechende Sensibilisierungsmaßnahmen im KIT an. IT-Beauftragte und Administratoren nehmen mindestens an der Grundlagenschulung zur IT-Sicherheit kam KIT teil und geben die Informationen bedarfsgerecht innerhalb ihres Wirkungsbereichs in den OE weiter.

3.4.1 Beteiligte

Federführung: ITSB

3.4.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.198: »Sensibilisierung der Mitarbeiter für Informationssicherheit«
- M 2.312: »Konzeption eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit«
- M 3.5: »Schulung zu Sicherheitsmaßnahmen«
- M 3.11: »Schulung des Wartungs- und Administrationspersonals«
- M 3.26: »Einweisung des Personals in den sicheren Umgang mit IT«
- M 3.44: »Sensibilisierung des Managements für Informationssicherheit«
- M 3.46: »Ansprechpartner zu Sicherheitsfragen«
- M 3.47: »Durchführung von Planspielen zur Informationssicherheit«
- M 3.48: »Auswahl von Trainern oder Schulungsanbietern«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.8.2.2: "Information security awareness, education and training"

3.5 Kryptographie

Um Kommunikation kryptographisch zu sichern, wird innerhalb des KIT ein Zertifizierungsdienst betrieben. Durch eine Public-Key Infrastructure (PKI) wird die einfache Nutzung von X.509-Zertifikaten ermöglicht. Das KIT betreibt zwei Zertifizierungsstellen: die KIT-CA, die beim DFN-Verein ausgelagert ist, und die GridKA-CA. Beide Zertifizierungsstellen stellen X.509-Zertifikate aus, die jedoch für verschiedene Anwendungsgebiete geeignet sind.

3.5.1 Zertifizierungsstelle KIT-CA

Die KIT-CA ist die oberste allgemeine Zertifizierungsinstanz des KIT. Ihre Aufgabe ist die Förderung gesicherter Kommunikation über das Internet. Die KIT-CA stellt Benutzern und Serverbetreibern innerhalb des KIT digitale Zertifikate aus. Zertifikate für Server können verwendet werden, um Verbindungen zu Servern zu verschlüsseln (SSL/TLS). Zertifikate für Benutzer können verwendet werden, um E-Mails zu signieren oder zu verschlüsseln oder um sich als Benutzer gegenüber Servern zu authentifizieren.

Weitere Informationen zu dieser Dienstleistung des SCC sind unter dem URL http://www.scc.kit.edu/dienste/kit-ca.php zu finden.

3.5.2 Beteiligte

Federführung: SCC

3.5.3 Zertifizierungsstelle GridKA-CA

Die GridKa-CA stellt PKI für X.509-Benutzer-, Rechner- und Dienstzertifikate zur Verfügung. Die Dienste der GridKa-CA können sowohl von Wissenschaftlern und Forschern, die in Deutschland an nationalen oder internationalen Grid-Projekten arbeiten, als auch für Ressourcen und Dienste in Anspruch genommen werden.

Zertifikate werden im Grid-Umfeld zur Authentifikation verwendet und sind die Basis der Grid Security Infrastructure, die in der Grid-Middleware umgesetzt wird. Die Prüfung der Identität einer Person, die der Ausstellung eines Zertifikats vorausgeht, folgt internationalen Standards und wird durch die Registrierungsstellen (Registration Authorities) der GridKa-CA durchgeführt. Mit der Zertifizierungsrichtlinie (Certification Policy) und Zertifizierungsdurchführungsbestimmung (Certification Practice Statement) werden alle einschlägigen Verfahrensweisen der GridKa-CA veröffentlicht. Diese Informationen werden ebenso wie die Zertifikatsperrliste (Certificate Revocation List) und allgemeine Informationen für die Nutzer regelmäßig auf dem neuesten Stand gehalten. In der Zertifikatsperrliste werden alle gesperrten Zertifikate der GridKa-CA aufgeführt; sie wird regelmäßig von Grid-Sites weltweit heruntergeladen.

Weitere Informationen zu dieser Dienstleistung des SCC sind unter dem URL: http://www.scc.kit.edu/dienste/5781.php zu finden.

3.5.4 Beteiligte

Federführung: SCC

3.5.5 Verschlüsselung von Anmeldedaten

Auf den Servern des KIT werden zum Schutz gegen das Ausspähen von Benutzerdaten alle Verbindungen verschlüsselt, über die sensible Daten gesendet werden. Um dies zu erreichen, existiert innerhalb des KIT die Richtlinie zur Nutzung von Verzeichnisdiensten des SCC, die in diesem Zusammenhang den Einsatz von Verschlüsselung verbindlich vorschreibt.

Diese und weitere Richtlinien sind verfügbar unter dem URL http://www.scc.kit.edu/dienste/sicherheitsrichtlinien.php.

3.5.6 Beteiligte

Federführung: SCC

3.5.7 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 2.46:** »Geeignetes Schlüsselmanagement«
- **M 2.162:** »Bedarfserhebung für den Einsatz kryptografischer Verfahren und Produkte«
- **M 2.163:** »Erhebung der Einflussfaktoren für kryptografische Verfahren und Produkte«
- **M 4.86:** »Sichere Rollenteilung und Konfiguration der Kryptomodule«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.11.5.1:** "Secure log-on procedures"
- **A.12.3.2:** "Key management"

3.6 Mobile Geräte

Um das Risiko eines Datenverlustes bei Benutzung von mobilen Geräten wie etwa PDAs, Smartphones oder Notebooks zu verringern, sind Regeln zu beachten. Häufig tritt Datenverlust durch Diebstahl eines Geräts auf. Neben dem unmittelbaren Verlust des Geräts kommt erschwerend hinzu, dass die Daten, die sich auf dem Gerät befunden haben, durch den Täter eingesehen und missbräuchlich genutzt werden können.

Die Richtlinie zum Umgang mit mobilen Geräten des KIT ist in die Themenfelder »Maßnahmen zum Schutz vor Datendiebstahl«, »Maßnahmen zum Schutz vor Gerätemanipulation«, »Maßnahmen zum Schutz vor Angriffen auf die Kommunikation« und »Maßnahmen bei Außerbetriebnahme des Gerätes« gegliedert.

Diese und weitere Richtlinien sind verfügbar unter dem URL http://www.scc.kit.edu/dienste/sicherheitsrichtlinien.php.

3.6.1 Beteiligte

Federführung:	ITSB
Zusätzlich beteiligt:	SCC, ITB

3.6.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **B 2.10:** »Mobiler Arbeitsplatz«
- **B 5.14:** »Mobile Datenträger«
- **G 5.141:** »Datendiebstahl über mobile Datenträger«
- **G 5.142:** »Verbreitung von Schadprogrammen über mobile Datenträger«
- **M 1.61:** »Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes«
- **M 2.309:** »Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung«
- **M 2.401:** »Umgang mit mobilen Datenträgern und Geräten«
- **M 2.430:** »Sicherheitsrichtlinien und Regelungen für den Informationsschutz unterwegs«
- **M 3.60:** »Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.10.8.3:** "Physical media in transit"
- **A.11.7.1:** "Mobile computing and communications"
- **A.11.7.2:** "Teleworking"

3.7 Meldewesen für IT-Sicherheitsvorfälle

3.7.1 Meldepflicht

Um Schäden für das KIT und seine Mitglieder und Angehörige zu vermeiden, sind von allen Benutzern der Infrastruktur für digitale Informationsverarbeitung und Kommunikation (IuK-Infrastruktur) des KIT folgende IT-Sicherheitsvorfälle umgehend dem KIT-CERT zu melden. Das KIT-CERT ist per E-Mail unter cert@kit.edu sowie telefonisch unter +49 721 608-45678 und per Telefax unter +49 721 608-9-45678 erreichbar. Durch solche Meldungen kann eine schnelle und zuverlässige Lagefeststellung erfolgen.

Eine Meldepflicht besteht für folgende IT-Sicherheitsvorfälle:

- Einbruch von Hackern in IT-Systeme des KIT;
- Verbreitung oder Ausführung von Schadcode durch vom KIT betriebene IT-Systeme;
- Kompromittierung (Kontrollverlust über) oder Manipulation von Zugangsdaten, geschäftswichtigen oder personenbezogenen Daten;
- Verlust von elektronischen Geräten oder Datenträgern, auf denen geschäftswichtige oder personenbezogene Daten gespeichert sind;
- Erpressung oder Nötigung durch Drohung mit einem der obigen Tatbestände sowie
- Einbringen oder Betrieb von Geräten Dritter im KIT-Netz, sofern dadurch einer der obigen Tatbestände verwirklicht wird.

Gemeldete IT-Sicherheitsverstöße werden durch das KIT-CERT dokumentiert.

Der IT-Sicherheitsbeauftragte kann bei Bedarf eine Meldepflicht für weitere spezifische IT-Sicherheitsvorfälle temporär oder auf Dauer aussprechen. Über eine Meldepflicht informiert der IT-Sicherheitsbeauftragte mittels Rundschreiben an alle Mitarbeitenden sowie auf seiner Webseite unter `https://www.itsb.kit.edu`.

3.7.2 Freiwillige Meldung

Andere als die in unter 3.7.1 genannten Vorgänge, die geeignet sind, die IT-Sicherheit im KIT zu gefährden, können freiwillig gemeldet werden. Insbesondere ist es zur zeitnahen Eindämmung von Phishingwellen für das KIT-CERT hilfreich, möglichst rasch Kenntnis von Angriffen zu erhalten. Wenn möglich, sind daher Kopien von Phishingmails an das KIT-CERT zur Kenntnis zu schicken. Eine freiwillige Meldung von IT-Sicherheitsvorfällen ist beispielsweise in folgenden Fällen sinnvoll:

- Gezielte Phishingversuche auf Nutzer des KIT;
- Einbruchsversuche von Hackern in IT-Systeme des KIT sowie
- Versuche, unbefugtem Zugang zu geschäftswichtigen oder personenbezogenen Daten zu erlangen.

3.7.3 Beteiligte

Federführung:	ITSB
Zusätzlich beteiligt:	KIT-CERT, ITB, Nutzer

3.7.4 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.158: »Meldung von Schadprogramm-Infektionen«
- M 2.201: »Dokumentation des Sicherheitsprozesses«
- M 2.498: »Behandlung von Warn- und Fehlermeldungen«
- M 6.23: »Verhaltensregeln bei Auftreten von Schadprogrammen«
- M 6.58: »Etablierung einer Vorgehensweise zur Behandlung von Sicherheitsvorfällen«
- M 6.59: »Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen«
- M 6.65: »Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.13.1.1: "Reporting information security events"
- A.13.1.2: "Reporting security weaknesses"
- A.13.2.1: "Responsibilities and procedures"
- A.13.2.2: "Learning from information security incidents"
- A.13.2.3: "Collection of evidence"

3.8 Netzwerksicherheit

Das Netzwerk des KIT wird durch verschiedene Maßnahmen geschützt. Einerseits wird das interne KIT-Netzwerk (das KIT-Intranet) gegenüber dem externen Internet entkoppelt, andererseits wird auch das Intranet in organisatorisch sinnvoll voneinander getrennte und unterschiedlich gegeneinander abgeschottete Subnetze unterteilt. Zudem sind allgemeine Überwachungs- und Schutzmechanismen in Kraft.

Der Zugang zu den drahtlosen Netzwerken des KIT wird durch Zugangskontrollmechanismen abgesichert, um unbefugten Zugriff zu unterbinden.

3.8.1 Trennung des Internets vom KIT-Intranet

Das KIT-Intranet wird durch ein mehrstufiges Schutzkonzept gegen Angriffe von außen gehärtet. Alle Außenanbindungen werden durch netzbasierte Intrusion-Prevention-Systeme (IPS) geschützt, die sämtlichen eingehenden Netzverkehr, soweit technisch möglich, auf Bedrohungen hin untersuchen und gegebenenfalls blockieren. Zusätzlich wird der eingehende Datenverkehr durch eine Firewall geleitet, die nur Netzwerkpakete zu bestimmten Netzwerkports durchlässt. Betreiber von Diensten können hierbei bis auf wenige Ausnahmen die Freischaltung von Ports für den Zugriff von externen Netzwerken aus durch einfachen Antrag erwirken.

Der ausgehende Datenverkehr ist in der Regel nicht beschränkt. Ausnahmen hierfür bilden wenige Ports, für die ausgehender Verkehr im allgemeinen nicht zulässig ist. Ein Beispiel hierfür ist der Protokollport 25/tcp, über den E-Mail-Versand abgewickelt wird; über diesen Port dürfen lediglich die zentralen Mailserver nach außen kommunizieren, um Spamversand durch befallene Endnutzersysteme zu verhindern und so Schaden vom KIT abzuwenden.

Zusätzlich zum allgemeinen Zugriff von außen bietet das KIT seinen Mitgliedern die Möglichkeit, mit Hilfe eines Virtual Private Network (VPN) auf das KIT-Intranet im allgemeinen oder auch auf besonders geschützte Netzwerkbereiche im besonderen zuzugreifen, indem nach zusätzlicher Authentifizierung eine kryptographisch abgesicherte Verbindung vom Endgerät des Benutzers, das etwa zu Hause mit Hilfe eines DSL-Anschlusses Zugang zum Internet hat, zu den entsprechenden Servern des KIT aufgebaut wird, so dass auch interne Netzbereiche für den Nutzer auf sichere Weise frei zugänglich sind.

3.8.2 Trennung einzelner Netzbereiche voneinander

Das Intranet des KIT ist in organisatorisch sinnvolle Abschnitte gegliedert. Je nach Anwendungsfall sind diese Subnetze ebenfalls durch Firewalls voneinander getrennt; die genauen Regeln für die ein- und ausgehenden Datenströme werden von den jeweils zuständigen Organisationseinheiten in Zusammenarbeit mit dem SCC festgelegt.

3.8.3 Verkehrsüberwachung

Zum frühzeitigen Erkennen und Analysieren von unerwünschtem oder gefährlichem Netzwerkverkehr werden die Verkehrsdaten aller vom SCC betriebenen Router zentral gesammelt und datenschutzkonform ausgewertet. Die erhobenen Verkehrsdaten beinhalten darüber hinaus in der reaktiven Behandlung

von Sicherheitsvorfällen wertvolle Spuren, die die Aufklärung erkannter Einbrüche ermöglichen und die Chance bieten, weitere an einem Vorfall beteiligte Systeme zu identifizieren.

3.8.4 Zugangskontrolle zum drahtlosen Netzwerk

Das SCC betreibt auf dem Gelände des KIT ein drahtloses Netzwerk, um den Mitgliedern sowie berechtigten Gästen eine bequeme und zeitgemäße Verbindung zum Internet zu ermöglichen. Hierbei können Mitglieder des KIT mit Hilfe ihres KIT-Benutzerkontos über Authentifizierung gemäß 802.1x direkten Zugang in das KIT-Intranet erlangen; Gäste anderer akademischer Einrichtungen können in der Regel über landesweite beziehungsweise internationale Kooperationen wie BelWü-Roaming oder EduRoam über das KIT-WLAN Zugang zu ihren Heimateinrichtungen erhalten und auf diese Weise das Internet nutzen. Gäste, die über ein KIT-Benutzerkonto verfügen, können über Web-Authentifizierung Zugang zum Internet erhalten.

3.8.5 Beteiligte

Federführung: SCC

3.8.6 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 1.63:** »Geeignete Aufstellung von Access Points«
- **M 2.75:** »Geeignete Auswahl eines Application-Level-Gateways«
- **M 2.383:** »Auswahl eines geeigneten WLAN-Standards«
- **M 2.384:** »Auswahl geeigneter Kryptoverfahren für WLAN«
- **M 2.385:** »Geeignete Auswahl von WLAN-Komponenten«
- **M 2.417:** »Planung der technischen VPN-Realisierung«
- **M 2.419:** »Geeignete Auswahl von VPN-Produkten«
- **M 4.82:** »Sichere Konfiguration der aktiven Netzkomponenten«
- **M 4.113:** »Nutzung eines Authentisierungsservers bei Remote-Access-VPNs«
- **M 4.294:** »Sichere Konfiguration der Access Points«
- **M 4.296:** »Einsatz einer geeigneten WLAN-Management-Lösung«
- **M 4.297:** »Sicherer Betrieb der WLAN-Komponente«
- **M 4.320:** »Sichere Konfiguration eines VPNs«
- **M 4.321:** »Sicherer Betrieb eines VPNs«
- **M 5.2:** »Auswahl einer geeigneten Netz-Topologie«
- **M 5.13:** »Geeigneter Einsatz von Elementen zur Netzkopplung«
- **M 5.60:** »Auswahl einer geeigneten Backbone-Technologie«
- **M 5.61:** »Geeignete physikalische Segmentierung«
- **M 5.62:** »Geeignete logische Segmentierung«
- **M 5.71:** »Intrusion Detection und Intrusion Response Systeme«
- **M 5.76:** »Einsatz geeigneter Tunnel-Protokolle für die VPN-Kommunikation«
- **M 5.77:** »Bildung von Teilnetzen«

- M 5.122: »Sicherer Anschluss von Laptops an lokale Netze«
- M 5.138: »Einsatz von RADIUS-Servern«
- M 5.139: »Sichere Anbindung eines WLANs an ein LAN«
- M 5.148: »Sichere Anbindung eines externen Netzes mit OpenVPN«
- M 5.149: »Sichere Anbindung eines externen Netzes mit IPSec«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.6.1: "Network controls"
- A.10.6.2: "Security of network services"
- A.11.4.1: "Policy on use of network services"
- A.11.4.2: "User authentication for external connections"
- A.11.4.5: "Segregation of networks"
- A.11.4.6: "Network connection control"
- A.11.4.7: "Network routing control"

3.9 Notfallvorsorge

Notfallvorsorge obliegt am KIT der Dienstleistungseinheit »Sicherheit und Umwelt« (SUM). SUM gewährleistet die radiologische und konventionelle technische Sicherheit sowie den Werkschutz des KIT und sorgt für die Umsetzung und Einhaltung gesetzlicher Vorgaben im Kontext des Umweltschutzes.

SUM steht unter der Leitung des vom Präsidium bestellten Sicherheitsbeauftragten des KIT, der im Rahmen seiner Dienstanweisung für das KIT die Umsetzung und Einhaltung sicherheitstechnischer Anforderungen überwacht. SUM stellt mit dem KIT-Informations-System Sicherheit (KISS) elektronische Dokumente zu den relevanten Themengebieten unter dem URL http://www.kiss.kit.edu/index.php bereit. Die IT-relevanten Aspekte der Notfallvorsorge, die den Wiederanlauf von Diensten nach Katastrophen oder Planungen einer Betriebskontinuität von zentralen Diensten definieren, werden vom SCC umgesetzt. Für Dienste, die innerhalb weiterer Organisationseinheiten erbracht werden, sind diese Planungen von den Verantwortlichen der Einheiten selbst umzusetzen.

3.9.1 Beteiligte

Federführung:	SUM
Zusätzlich beteiligt:	SCC, ITB

3.9.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **M 6.33:** »Entwicklung eines Datensicherungskonzepts«
- **M 6.110:** »Festlegung des Geltungsbereichs und der Notfallmanagementstrategie«
- **M 6.111:** »Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene«
- **M 6.112:** »Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement«
- **M 6.113:** »Bereitstellung angemessener Ressourcen für das Notfallmanagement«
- **M 6.114:** »Erstellung eines Notfallkonzepts«
- **M 6.115:** »Integration der Mitarbeiter in den Notfallmanagement-Prozess«
- **M 6.116:** »Integration von Notfallmanagement in organisationsweite Abläufe und Prozesse«
- **M 6.117:** »Tests und Notfallübungen«
- **M 6.118:** »Überprüfung und Aufrechterhaltung der Notfallmaßnahmen«
- **M 6.119:** »Dokumentation im Notfallmanagement-Prozess«
- **M 6.120:** »Überprüfung und Steuerung des Notfallmanagement-Systems«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.9.1.1:** "Physical Security Perimeter"
- **A.9.1.2:** "Physical Entry Controls"
- **A.9.1.3:** "Securing rooms, offices and facilities"
- **A.9.1.4:** "Protecting against external and environmental threats"

- A.9.1.5: "Working in secure areas"
- A.9.1.6: "Public access, delivery and loading area"

3.10 Passwörter

Der Zugang zu Rechenanlagen, Diensten und Teilen der Benutzerdaten innerhalb des KIT wird mittels personalisierten Zugangsdaten (Benutzerkennung und Passwort) geregelt und geschützt. Ein sorgfältiger Umgang mit Passwörtern ist unerlässlich.

Die Passwortrichtlinie des KIT legt nur die minimalen KIT-weit geltenden Passwortkriterien fest. Darüber hinaus gehende Verschärfungen der Passwortkriterien können von den IT-Dienstebetreibern zusätzlich in Ihrem Verantwortungsbereich umgesetzt werden.

Der Einsatz und Umgang mit Passwörtern für KIT-Rechnersysteme und -Dienste wird in der Passwortrichtlinie des KIT geregelt. Diese ist in die Abschnitte »Auswahl von Passwörtern« und »Sensibler Umgang mit Passwörtern« gegliedert.

Die aktuelle Fassung der Passwortrichtlinie ist unter dem URL http://www.scc.kit.edu/dienste/sicherheitsrichtlinien.php verfügbar.

3.10.1 Beteiligte

Federführung:	ITSB
Zusätzlich beteiligt:	SCC, ITB

3.10.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- **G 3.43:** »Ungeeigneter Umgang mit Passwörtern«
- **G 5.18:** »Systematisches Ausprobieren von Passwörtern«
- **M 2.11:** »Regelung des Passwortgebrauchs«
- **M 2.22:** »Hinterlegen des Passwortes«
- **M 2.402:** »Zurücksetzen von Passwörtern«
- **M 4.1:** »Passwortschutz für IT-Systeme«
- **M 4.7:** »Änderung voreingestellter Passwörter«
- **M 4.14:** »Obligatorischer Passwortschutz unter Unix«
- **M 4.27:** »Zugriffsschutz am Laptop«
- **M 4.306:** »Umgang mit Passwort-Speicher-Tools«
- **M 5.34:** »Einsatz von Einmalpasswörtern«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- **A.11.2.3:** "User password management"
- **A.11.3.1:** "Password use"
- **A.11.3.2:** "Unattended user equipment"
- **A.11.5.2:** "User identification and authentication"

3.11 Patchmanagement

Sowohl Client- als auch Serversysteme müssen regelmäßig mit Patches und Updates der Betriebssystem- und Anwendungssoftware versorgt werden. Die Verwaltung der Sicherheitsupdates ist ein wesentlicher Bestandteil der IT-Administration, um Sicherheitsrisiken zu minimieren. Softwarehersteller stellen in der Regel Reparaturen – sogenannte Patches – für bekannte Sicherheitsprobleme zur Verfügung. Für einen sicheren Betrieb ist es unerlässlich, diese Patches zeitnah einzuspielen.

3.11.1 Beteiligte

Federführung:	SCC
Zusätzlich beteiligt:	ITB

3.11.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.221: »Änderungsmanagement«
- M 2.421: »Planung des Patch- und Änderungsmanagementprozesses«
- M 2.422: »Umgang mit Änderungsanforderungen«
- M 2.423: »Festlegung der Verantwortlichkeiten für das Patch- und Änderungsmanagement«
- M 2.424: »Sicherheitsrichtlinie zum Einsatz von Patch- und Änderungsmanagement-Werkzeugen«
- M 2.425: »Geeignete Auswahl von Werkzeugen für das Patch- und Änderungsmanagement«
- M 2.426: »Integration des Patch- und Änderungsmanagements in die Geschäftsprozesse«
- M 4.324: »Konfiguration von Autoupdate-Mechanismen beim Patch- und Änderungsmanagement«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.1.1: "Documentation of operating procedures"
- A.10.1.2: "Change Management"

3.12 Personal-/Identitätsmanagement

Das Personal im KIT nutzt IT-Ressourcen zur Erfüllung seiner Aufgaben. Die verschiedenen Nutzergruppen im KIT werden identifiziert, so dass entsprechende IT-Ressourcen rollenbezogen zur Verfügung gestellt werden können. Ebenso ist neben der Rolle der IT-Nutzer auch die Rolle der IT-Betreiber bzw. IT-Dienstebetreiber zu identifizieren. Nach Identifikation der Rollen müssen diese in den nachgelagerten Systemen zur Verfügung stehen, was möglichst durch das zentrale Identitätsmanagement umzusetzen ist.

3.12.1 Beteiligte

Federführung:	ASDUR
Zusätzlich beteiligt:	IT-Dienstbetreiber, SCC, ITB

3.12.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.226: »Regelungen für den Einsatz von Fremdpersonal«
- M 3.1: »Geregelte Einarbeitung/Einweisung neuer Mitarbeiter«
- M 3.5: »Schulung zu Sicherheitsmaßnahmen«
- M 3.6: »Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern«
- M 3.10: »Auswahl eines vertrauenswürdigen Administrators und Vertreters«
- M 3.11: »Schulung des Wartungs- und Administrationspersonals«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.8.1.1: "Roles and responsibilities"
- A.8.1.2: "Screening"
- A.8.1.3: "Terms and conditions of employment"
- A.8.3.1: "Termination responsibilities"
- A.8.3.2: "Return of assets"
- A.8.3.3: "Removal of access rights"
- A.11.2.1: "User registration"
- A.11.2.2: "User privilege management"
- A.11.2.3: "User password management"
- A.11.2.4: "Review of user access rights"
- A.11.5.2: "User identification and authentication"
- A.11.5.2: "Password management system"

3.13 Schutz vor Schadprogrammen

Das Computer-Virenschutzkonzept ist für das KIT über die Bereitstellung einer einheitlichen Plattform umgesetzt. Alle Rechner des KIT können am zentralen Anti-Viren-Management (AV-Management) des KIT teilnehmen.

3.13.1 Beteiligte

Federführung: SCC
Zusätzlich beteiligt: ITB

3.13.2 Virenschutz für Mailserver

Die Mailserver des KIT, die vom SCC betrieben werden, verwenden Virenscanner unterschiedlicher Hersteller, um den Anwendern einen möglichst großen Schutz vor Viren, die per E-Mail verschickt werden, zu bieten.

3.13.3 Beteiligte

Federführung: SCC

3.13.4 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.154: »Erstellung eines Sicherheitskonzeptes gegen Schadprogramme«
- M 2.157: »Auswahl eines geeigneten Viren-Schutzprogramms«
- M 2.158: »Meldung von Schadprogramm-Infektionen«
- M 2.159: »Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen«
- M 2.160: »Regelungen zum Schutz vor Schadprogrammen«
- M 2.224: »Vorbeugung gegen Schadprogramme«
- M 4.3: »Einsatz von Viren-Schutzprogrammen«
- M 5.69: »Schutz vor aktiven Inhalten«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.10.4.1: "Controls against malicious code"
- A.10.4.2: "Controls against malicious mobile code"
- A.10.5.1: "Information back-up"

3.14 Schwachstellenmanagement

Schwachstellenmanagement beschreibt den Prozess des Aufspürens, Nachverfolgens und Beseitigens von Schwachstellen an und in Netzwerk- oder Rechnersystemen. Um diesen Prozess nachhaltig umzusetzen, betreibt das SCC innerhalb des KIT Systeme, deren Aufgabe es ist, Schwachstellen aufzuspüren. Werden Schwachstellen gefunden, so werden die Verantwortlichen der Rechnersysteme kontaktiert, um für eine zügige Behebung zu sorgen.

3.14.1 Beteiligte

Federführung:	SCC
Zusätzlich beteiligt:	IT-Dienstbetreiber

3.14.2 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.35: »Informationsbeschaffung über Sicherheitslücken des Systems«
- M 4.25: »Einsatz der Protokollierung im Unix-System«
- M 4.93: »Regelmäßige Integritätsprüfung«
- M 5.8: »Regelmäßiger Sicherheitscheck des Netzes«
- M 5.9: »Protokollierung am Server«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.6.1.7: "Contact with special interest groups"
- A.7.1.1: "Inventory of assets"
- A.7.1.2: "Ownership of assets"
- A.10.4.1: "Controls against malicious software"
- A.10.6.1: "Network controls"
- A.10.9.3: "Publicly available information"
- A.10.10.3: "Protection of log information"
- A.10.10.4: "Administrator and operator logs"
- A.12.6.1: "Control of technical vulnerabilities"
- A.13.1.2: "Reporting security weaknesses"

3.15 Zutrittsregelung Serverräume

Ein Serverraum dient in erster Linie zur Unterbringung von Servern und Maschinen. Darüber hinaus können dort serverspezifische Unterlagen, Datenträger in kleinem Umfang oder weitere Hardware (etwa Sternkoppler, Protokolldrucker, Klimatechnik) vorhanden sein.

In einem Serverraum ist kein ständig besetzter Arbeitsplatz eingerichtet, er wird nur sporadisch und zu kurzfristigen Arbeiten betreten. Zu beachten ist jedoch, dass im Serverraum aufgrund der Konzentration von IT-Geräten und Daten ein deutlich höherer Schaden eintreten kann als zum Beispiel in einem Büroraum. Nur diejenigen Personen, die zur Durchführung ihrer Aufgaben direkten Zugriff auf Server und sonstige im Serverraum installierte Geräte wie Kommunikationsverteiler, Firewalls und so fort benötigen, erhalten Zutritt zu einem Serverraum. In Serverräumen gilt Rauchverbot.

Serverräume sind grundsätzlich immer verschlossen, wenn sie nicht besetzt sind. Der Zugang zu Rechnerräumen ist durch ein Schlüsselsystem mit einem entsprechenden Autorisierungs- und Authentifizierungsverfahren für berechtigte Personen geschützt.

3.15.1 Zugangsregelung zu Serverräumen des zentralen IT-Dienstleisters SCC

Der Sicherheitsbereich des SCC umfasst alle vom SCC betreuten Rechnerräume im Campus Süd und Campus Nord. Die KITCard wird als Zugangskarte verwendet.

3.15.2 Beteiligte

Federführung:	SCC
Zusätzlich beteiligt:	ITB

3.15.3 Referenzen

BSI-Referenz

Die Maßnahmen entsprechen den folgenden Maßnahmen der BSI-Kataloge (14. Ergänzungslieferung):

- M 2.6: »Vergabe von Zutrittsberechtigungen«
- M 2.17: »Zutrittsregelung und -kontrolle«
- M 2.220: »Richtlinien für die Zugriffs- bzw. Zugangskontrolle«

ISO-27001-Referenz

Die Maßnahmen entsprechen den folgenden Control Objects von ISO 27001:2015:

- A.9.1.5: "Working in secure areas"
- A.9.1.6: "Public access, delivery and loading areas"