Karlsruher Institut für Technologie

IT-Sicherheit am KIT

Leitlinie des Karlsruher Instituts für Technologie

PRÄSIDIUM

KIT – Universität des Landes Baden-Württemberg und
nationales Forschungszentrum in der Helmholtz-Gemeinschaft

www.kit.edu

Karlsruher Institut für Technologie

Präambel

Die Leistungsfähigkeit des Karlsruher Instituts für Technologie (KIT) hängt maßgeblich von der Verfügbarkeit und Qualität der Dienste der Informationstechnik (IT) ab. Gleichwohl ist die IT-Infrastruktur immer stärkeren Gefahren ausgesetzt. Die Ergreifung von Schutzmaßnahmen zur Sicherstellung aller IT-gestützten Dienste in Forschung, Innovation, Studium und Lehre, Weiterbildung und Verwaltung am KIT besitzt daher höchste Priorität.

Diese Leitlinie beschreibt den Informationssicherheitsprozess für das KIT und dient als Grundlage für ein IT-Sicherheitskonzept. Die daraus resultierenden Maßnahmen sollen eine größtmögliche Sicherheit im Bereich der Informationstechnik gewährleisten. Diese Sicherheit ist unabdingbare Voraussetzung für Datenschutzmaßnahmen, die insbesondere bei der Verarbeitung personenbezogener Daten zu gewährleisten sind. Eine erfolgreiche Umsetzung des IT-Sicherheitsprozesses setzt geregelte Verantwortungsstrukturen sowie die Unterstützung aller Mitglieder des KIT voraus.

Die IT-Sicherheitspolitik am KIT 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 miteinander vereinbaren lassen.

Geltungsbereich

Diese Leitlinie gilt für alle Einrichtungen des KIT, für dessen gesamte IT-Infrastruktur einschließlich der betriebenen IT-Systeme und aller am KIT-weiten Netzwerk angeschlossenen Geräte, sowie für die in der IuK-Ordnung des KIT definierten Nutzer.

Karlsruher Institut für Technologie

Zielsetzungen

Die anzustrebenden Schutzziele sind:

- die Verfügbarkeit der Infrastruktur und der Daten,
- die Vertraulichkeit der Daten vor unautorisiertem Zugriff,
- die Integrität der Daten.

Das KIT schützt 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,
- Wahrung der Persönlichkeitsrechte der Mitglieder und der Angehörigen.

Karlsruher Institut für Technologie

Organisation

Die nachfolgenden Personen und Gremien spielen im IT-Sicherheitsprozess des KIT eine tragende Rolle:

- **Das Präsidium des Karlsruher Instituts für Technologie und der CIO**
  Das Präsidium des KIT trägt die Gesamtverantwortung für die IT-Sicherheit am KIT. Der Chief Information Officer (CIO) des KIT ist für Fragen der IT-Sicherheit zuständig.

- **Der Ausschuss für Informationsverarbeitung und -versorgung (IV-A)**
  Dieser vom Senat und dem Präsidium eingesetzte und vom CIO geleitete Ausschuss gibt Senat und Präsidium Empfehlungen in allen die Bereiche Informationsversorgung und -verarbeitung am KIT betreffenden Fragen von allgemeiner und grundsätzlicher Bedeutung, also auch in Fragen der IT-Sicherheit.

- **Der IT-Sicherheitsbeauftragte des Karlsruher Instituts für Technologie**
  Der IT-Sicherheitsbeauftragte (ITSB) wird vom Präsidium des KIT durch das Direktorium des Steinbuch Centre for Computing (SCC) bestellt. Er ist Mitglied im Arbeitsstab ASDUR und berichtet direkt an den CIO des KIT. Der ITSB ist für die strategische Ausrichtung der IT-Sicherheit am KIT federführend. Er koordiniert diese Aufgabe sachbezogen und themenübergreifend in ASDUR.

- **Der Arbeitsstab IT-Sicherheit, Datenschutz und Recht (ASDUR)**
  ASDUR ist ein vom CIO des KIT geleiteter Arbeitsstab, der themenübergreifende Fragestellungen aus den Bereichen IT-Sicherheit, Datenschutz und IT-Compliance bearbeitet. ASDUR gehören sowohl Experten zu den Bereichen IT-Sicherheit, Datenschutz und IT-Compliance als auch Vertreter der Nutzergruppen an. Durch ASDUR erarbeitete Empfehlungen für strategische Richtlinien oder Regelungen erfahren durch den CIO im IV-A entsprechende Priorität zur weiteren Vorlage im KIT-Präsidium.

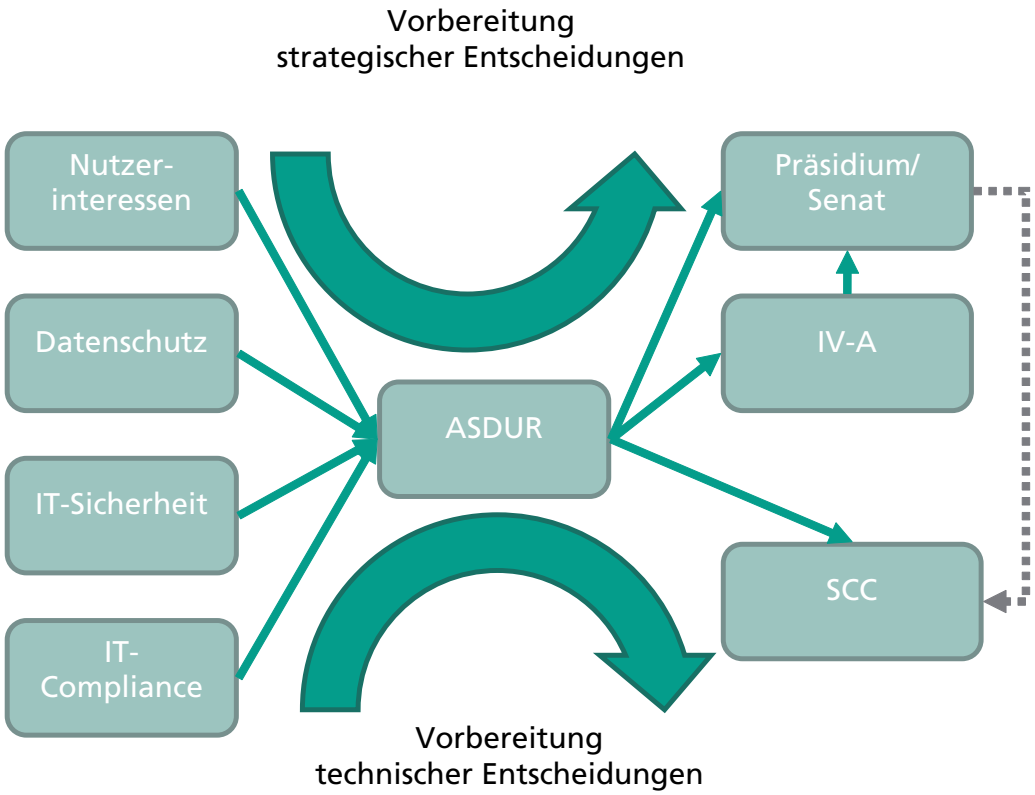
- **Das SCC und das Computernotfallteam des KIT (KIT-CERT)**
  Das SCC betreibt neben seinen Aufgaben im Forschungs-, Lehr- und Entwicklungsumfeld auch die zentralen IT-Dienste des KIT. Es ist neben dem Betrieb dieser Dienste für die Umsetzung der sicherheitstechnischen Maßnahmen am KIT verantwortlich. Überdies erarbeitet das SCC Leitfäden und Dokumentationen für die Nutzer des KIT und stellt diese zur Verfügung. Die Nutzer des KIT werden durch Mitarbeiter des SCC in die für sie relevanten IT-Sicherheitsmaßnahmen unterwiesen und auf die konsequente Anwendung derselben verpflichtet. Das KIT-CERT ist die zentrale Koordinationsstelle des KIT bei Missbrauch von IT-Diensten oder Anlagen. Es ist als Teil des SCC sehr nah an den technischen Systemen und hat direkten Kontakt zu den verantwortlichen Mitarbeitern, um eine zügige Bearbeitung von Vorfällen zu gewährleisten.

- **Die IT-Verantwortlichen der Organisationseinheiten und die Nutzer**
  Die IT-Verantwortlichen der Organisationseinheiten und die Nutzer setzen die Richtlinien des KIT in den Organisationseinheiten um und sind dort Ansprechpartner für alle IT-relevanten Aspekte.

Karlsruher Institut für Technologie

IT-Sicherheitsprozess am KIT

Das nachfolgende Diagramm skizziert den IT-Sicherheitsprozess am KIT. Es ist ausdrücklich kein Weisungsgefüge dargestellt.



Es ist zu sehen, dass das Schaubild in drei vertikale Abschnitte unterteilbar ist: Links sind die Themenkomplexe aufgeführt, die für die Umsetzung von sicherheitsrelevanten Fragestellungen bei IT-Lösungen für KIT zu betrachten sind. In der Mitte ist als zentraler operativer Arbeitsstab ASDUR platziert, dieser erörtert Fragestellungen im Kontext des Datenschutzes sowie der rechtlichen Lage. Als Ergebnis werden Entscheidungsvorlagen und Begutachtungen für die Leitung des KIT erstellt. Aufgrund seiner Aufgabe und seines Charakters kann ASDUR diese Entscheidungen und Richtlinien nicht selbst verabschieden, sondern macht Ergebnisse den übergeordneten Gremien zur Verabschiedung bzw. dem SCC und anderen zentralen Einrichtungen (z. B. Bibliothek) zur technischen Umsetzung bekannt. Im Schaubild ist zudem noch der Kommunikationsweg der strategischen Entscheidungen vom Präsidium zum SCC (stellvertretend für die zentralen Einrichtungen) rechts aufgeführt.

Karlsruher Institut für Technologie

Sachverwandte Themen im IT-Sicherheitsprozess

Datenschutz am KIT
Die Bereitstellung von IT-Infrastruktur und IT-Dienstleistungen am KIT und durch das KIT bedingt die Verarbeitung personenbezogener Daten. Dabei ist das Grundrecht auf informationelle Selbstbestimmung der Betroffenen zu wahren. Deshalb ist der Zulässigkeit, der Erforderlichkeit, der Zweckbindung der Daten, sowie der Datensparsamkeit und der Datenvermeidung bei allen Verarbeitungsvorgängen, insbesondere bei Telekommunikations- und Telemediendiensten besondere Aufmerksamkeit zu widmen.

Für die jeweiligen Verfahren sind die rechtlichen Regelungen und die technisch-organisatorischen Maßnahmen mittels eines Verfahrensverzeichnisses zu erfassen und gegebenenfalls erforderliche Vorabkontrollen durchzuführen.

Hierbei sind die Gesichtspunkte des Datenschutzes bereits bei der Konzeption von Vorhaben, bei denen personenbezogene Daten automatisch verarbeitet werden, mit einzubeziehen. Die Mitarbeiter des KIT sind im Bezug auf den Datenschutz zu informieren, zu schulen und zu sensibilisieren.

IT-Compliance am KIT
Ziel der IT-Compliance am KIT ist die umfassende und dauerhafte Sicherstellung der Einhaltung der für das KIT anwendbaren gesetzlichen und vertraglichen Regelungen, Rechtsverordnungen, Verwaltungsvorschriften und internen Richtlinien, die für die IT gelten. Aus diesen Vorgaben sind konkrete Anforderungen an die IT zu entwickeln. Zum Erreichen dieses Zieles ist die Analyse und Bewertung der bestehenden Prozesse am Karlsruher Institut für Technologie und die Dokumentation entsprechend anzuwendender Regelungen und Richtlinien erforderlich. Anschließend sind wirksame Maßnahmen zu erarbeiten, die einen rechtskonformen und verantwortungsvollen Umgang aller IT-Aspekte sichern und erkennbare Defizite beseitigen. Besondere Bedeutung kommt hierbei der Datensicherheit, der Verfügbarkeit, der Vertraulichkeit und dem Datenschutz zu.

Inkrafttreten
Diese Leitlinie wurde vom Präsidium des KIT verabschiedet und tritt zum 1.10.2009 in Kraft.

Herausgeber
Karlsruher Institut für Technologie (KIT)
Präsidium
Kaiserstraße 12 | 76131 Karlsruhe

Stand November 2009

www.kit.edu