

AMTLICHES MITTEILUNGSBLATT

Herausgeber: Der Präsident der Technischen Universität Berlin
Straße des 17. Juni 135, 10623 Berlin
ISSN 0172-4924

Nr. 18/2016
(69. Jahrgang)

Redaktion: Ref. K 3, Telefon: 314-22532

Berlin, den
2. August 2016

INHALT

II. Bekanntmachungen

Seite

Präsidium

IT-Sicherheitsleitlinie

vom 7. Juli 2016..... 168

II. Bekanntmachungen

Präsidium

IT-Sicherheitsleitlinie

vom 7. Juli 2016

Präambel

Die Informationstechnik bestimmt in maßgeblichem Umfang die Leistungsfähigkeit der Technischen Universität Berlin. Besonders die Verfügbarkeit und die Qualität der Dienste ist ausschlaggebend für qualitativ hochwertige Forschung und Lehre. 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 an der TU Berlin besitzt daher höchste Priorität.

Diese Leitlinie beschreibt die Zielsetzungen des gesamten IT-Sicherheitsprozesses 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 der TU Berlin voraus.

Die IT-Sicherheitspolitik der TU Berlin 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.

Geltungsbereich

Diese Leitlinie gilt für alle Einrichtungen der TU Berlin, für deren gesamte IT-Infrastruktur einschließlich der betriebenen IT-Systeme und aller am TU-weiten Netzwerk angeschlossenen Geräte sowie für alle Mitglieder der Hochschule.

Zielsetzungen

Die anzustrebenden Schutzziele sind:

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

Die TU Berlin schützt ihre Interessen und ihr Ansehen in der Öffentlichkeit durch die Sicherung ihrer Arbeitsfähigkeit, Vertrauenswürdigkeit und Zuverlässigkeit.

Zu den IT-Sicherheitszielen der TU Berlin zählen:

- die Gewährleistung der Verfügbarkeit der IT-Systeme, Programme und Daten,
- die Transparenz und die Nachhaltigkeit muss gewährleistet sein,
- 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,
- die Wahrung der Persönlichkeitsrechte der Mitglieder und Angehörigen der TU Berlin.

Organisation

Die nachfolgenden Personen und Gremien spielen im IT-Sicherheitsprozess der TU Berlin eine tragende Rolle:

- **Das Präsidium der Technischen Universität Berlin und die/der CIO**

Das Präsidium der TU Berlin trägt die Gesamtverantwortung für die IT-Sicherheit an der TU Berlin. Die/der Chief Information Officer (CIO) der TU Berlin ist für Fragen der IT-Sicherheit zuständig.

- **Der Beirat für Informationsverarbeitung und -versorgung (IV-Beirat)**

Dieser von der/dem CIO geleitete Ausschuss gibt dem Akademischen Senat und Präsidium Empfehlungen in allen die Bereiche Informationsverarbeitung und -versorgung an der TU Berlin betreffenden Fragen von allgemeiner und grundsätzlicher Bedeutung, also auch in Fragen der IT-Sicherheit.

- **Die/der IT-Sicherheitsbeauftragte der TU Berlin**

Die/der IT-Sicherheitsbeauftragte (ITSB) wird vom Präsidium der TU Berlin bestellt. Sie/er ist Mitglied im IT-Sicherheitsboard und berichtet direkt an die/den CIO der TU Berlin. Die/der ITSB ist für die strategische Ausrichtung der IT-Sicherheit an der TU Berlin federführend. Sie/er koordiniert diese Aufgabe sachbezogen und themenübergreifend im IT-Sicherheitsboard.

- **Das IT-Sicherheitsboard der TU Berlin**

Das IT-Sicherheitsboard ist ein von der/dem CIO der TU Berlin geleiteter Arbeitsstab, der themenübergreifende Fragestellungen aus den Bereichen IT-Sicherheit, Datenschutz und IT-Compliance bearbeitet. Dem Board gehören sowohl Expertinnen und Experten zu den Bereichen IT-Sicherheit, Datenschutz und IT-Compliance als auch Vertreterinnen und Vertreter der Nutzergruppen an. Durch das Board erarbeitete Empfehlungen für strategische Richtlinien oder Regelungen erfahren durch die/den CIO im IV-Beirat entsprechende Priorität zur weiteren Vorlage im Präsidium der TU Berlin.

- **Das IT-Service Center tubIT und das Computernotfallteam (TUB-CERT)**

tubIT betreibt die zentralen IT-Dienste der TU Berlin. Es ist neben dem Betrieb dieser Dienste für die Umsetzung der sicherheitstechnischen Maßnahmen an der TU Berlin verantwortlich. Überdies erarbeitet tubIT Leitfäden und Dokumentationen für seine Nutzerinnen und Nutzer und stellt diese zur Verfügung.

Die Nutzerinnen und Nutzer der IT-Dienste der TU Berlin werden durch tubIT-Mitarbeiterinnen und -Mitarbeiter in den für sie relevanten IT-Sicherheitsmaßnahmen unterwiesen und auf die konsequente Anwendung derselben verpflichtet. Das TUB-CERT ist die zentrale Koordinationsstelle der TU Berlin bei Missbrauch von IT-Diensten oder Anlagen. Es ist als Teil von tubIT sehr nah an den technischen Systemen und hat direkten Kontakt zu den verantwortlichen Mitarbeiterinnen und Mitarbeitern, um eine zügige Bearbeitung von Vorfällen zu gewährleisten.

- **Die IT-Verantwortlichen der Organisationseinheiten und die Nutzer**

Die IT-Verantwortlichen der Organisationseinheiten (entsprechend der hierarchischen Organisationsstruktur der TU Berlin) und die Nutzerinnen und Nutzer setzen die Richtlinien der TU Berlin in den Organisationseinheiten um und sind dort Ansprechpartner für alle IT-relevanten Aspekte.

Sachverwandte Themen im IT-Sicherheitsprozess

Datenschutz an der TU Berlin

Die Bereitstellung von IT-Infrastruktur und IT-Dienstleistungen an der TU Berlin und durch die TU Berlin 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 Verfahrensverzeichnis 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 Mitarbeiterinnen und Mitarbeiter der TU Berlin sind in Bezug auf den Datenschutz zu informieren, zu schulen und zu sensibilisieren.

IT-Compliance an der TU Berlin

Ziel der IT-Compliance an der TU Berlin ist die umfassende und dauerhafte Sicherstellung der Einhaltung der für die TU Berlin 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 an der TU Berlin 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 der TU Berlin verabschiedet und tritt mit Erscheinen im Amtlichen Mitteilungsblatt der TU Berlin in Kraft.