IT-Sicherheitsleitlinie der Universität Bayreuth

Präambel

Für die Universität Bayreuth ist die Informations- und Kommunikationstechnik von zentraler Bedeutung für die Aufgabenerfüllung in Forschung und Lehre. Das Spektrum der IT-Anwendungen umfasst den Betrieb von Anlagen, die Durchführung von Versuchen und Experimenten, wissenschaftliche Anwendungen und Simulationen, die Lehre, die Arbeit in der Verwaltung sowie der Zentralen Dienste und die Kommunikation mit externen Partnern und Auftraggebern.

Die Sicherheit in der Informationstechnik sowie die Einhaltung der datenschutzrechtlichen und gesetzlichen Bestimmungen sind eine grundlegende Voraussetzung für eine funktionsfähige Infrastruktur der Universität. Sie zu gewährleisten ist Aufgabe aller Einrichtungen der Universität und der Nutzer der IT-Infrastruktur.

Die IT-Sicherheitsleitlinie ergänzt die „Ordnung für die Informationsverarbeitungs-Infrastruktur der Universität Bayreuth“ vom 10. Februar 2005.

Die IT-Sicherheit an der Universität Bayreuth orientiert sich am Grundverständnis des Bundesamtes für Sicherheit der Informationstechnik (BSI) zur IT-Sicherheit.

§1 Gegenstand der IT-Sicherheitsleitlinie und Begriffsbestimmungen

Die vorliegende Leitlinie legt Zuständigkeiten, Pflichten und Aufgaben sowie Regelungen zur Finanzierung im Bereich der IT-Sicherheit fest.

Im Sinne dieser Leitlinie ist

1. "Sicherheit in der Informationstechnik" (IT-Sicherheit):
   Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme der Universität (z.B. PC-Arbeitsplatz, E-Mail, elektronische Bibliotheken, Prüfungsverwaltung, Hochleistungsrechner, Gesamtheit der IT-Verfahren der Universität) sowie der Datenbestände.
2. "Verfügbarkeit":
   Ein Zustand, in dem Daten, Dienste und Funktionen eines IT-Systems und seiner Komponenten von den berechtigten Personen zum geforderten Zeitpunkt in der vorgesehenen Zeit sowie in der gesicherten Form und Qualität nutzbar sind.
3. "Integrität":
   Ein manipulationsfreier Zustand von Daten und IT-Systemen.
4. "Vertraulichkeit":
   Ein Zustand, in dem die Nutzung von Daten nur berechtigen Personen in zulässiger Weise möglich ist.

5. "IT-Infrastruktur":
   Gesamtheit der Hardware, Anwendungen und baulichen Einrichtungen der Universität, die der Informationsverarbeitung dienen.
6. "IT-System":
   Die funktionelle Einheit aus Hard-und Software, die Daten erhebt, erfasst, aufbereitet, nutzt, speichert, übermittelt, programmgesteuert verarbeitet, intern darstellt, ausgibt und wiedergewinnt.
7. „IT-Sicherheitsprozess“:
   Die Gesamtheit der Verfahren, die das Ziel haben, IT-Sicherheit in alle Abläufe der Universität zu integrieren, um eine konstante Weiterentwicklung und Verbesserung der IT-Sicherheit zu gewährleisten.

§2 Geltungsbereich

Die IT-Sicherheitsleitlinie gilt für alle Personen und Systeme, die die IT-Infrastruktur der Universität Bayreuth nutzen.

§3 Grundpflichten

(1) Alle Nutzer der mit der IT-Infrastruktur der Universität Bayreuth verbundenen IT-Systeme sind verpflichtet, auf IT-Sicherheit hinzuwirken und die dazu erforderlichen Maßnahmen zu treffen.
(2) Die Verantwortlichkeit für IT-Sicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme.
(3) Alle Nutzer haben die Pflicht, Ereignisse, die die IT-Sicherheit beeinträchtigen oder beeinträchtigen könnten, unverzüglich nach Kenntniserlangung dem IT-Servicezentrum zu melden. Das IT-Servicezentrum setzt anschließend den IT-Sicherheitsbeauftragten (IT-SB) in Kenntnis.

§4 Beteiligte am IT-Sicherheitsprozess und deren Aufgaben

(1) Hochschulleitung

Die Gesamtverantwortung für die Gewährleistung der IT-Sicherheit und die Einhaltung des IT-Sicherheitsprozesses an der Universität Bayreuth liegt bei der Hochschulleitung.

Der **Chief Information Officer (CIO)** nimmt als Mitglied der Hochschulleitung die, die Universität in ihrer Gesamtheit betreffenden, Koordinierungsaufgaben im Bereich IT-Sicherheit nach Rücksprache mit dem IT-Sicherheitsbeauftragten (IT-SB) wahr.

(2) Präsidialkommission Informations- und Kommunikationstechnologien (PK IKT)

Die PK IKT erarbeitet für den Bereich Informations- und Kommunikationstechnologien strategische Vorschläge als Entscheidungsgrundlage für die Hochschulleitung. Ergebnisse des, der PK IKT untergeordneten, Arbeitskreises IT-Sicherheit werden der PK IKT berichtet. Nach

Beschluss werden diese gegebenenfalls zur Genehmigung bzw. Inkraftsetzung an die Hochschulleitung weiterleitet.

(3) Arbeitskreis IT-Sicherheit (AK IT-Sicherheit)

Der AK IT-Sicherheit bereitet strategische Zielsetzungen und Entscheidungen im Bereich IT-Sicherheit für die PK IKT vor. Der Arbeitskreis initiiert, steuert und koordiniert den Informationssicherheitsprozess unter Mitwirkung des IT-SB. Dazu gehören u.a. alle die IT-Sicherheit betreffenden Themen.

(4) IT-Sicherheitsbeauftragter (IT-SB)

Der IT-SB wird von der Hochschulleitung ernannt. Der IT-SB ist ständiges Mitglied der PK IKT und des AK IT-Sicherheit.

Der IT-SB hat ein Informationsrecht und ein Vorschlagsrecht.

Das Informationsrecht des IT-SB wird u.a. durch die Teilnahme an den Hochschulgremien und Aufnahme in deren Informationsverteilern wahrgenommen. Darüber hinaus besteht ein aktives Informationsrecht für den IT-SB. Dieser kann auf die Protokolle von Hochschulleitung, Hochschulrat, Senat, Fakultätsräten und Niederschriften des IT-Servicezentrums etc. zugreifen, sofern sie die Themen IT-Infrastruktur und IT-Sicherheit betreffen.

Das Vorschlagsrecht des IT-SB dient dazu, eigene Vorschläge bezüglich der IT-Sicherheit an alle unter §4 genannten Beteiligten und Gremien sowie an Nutzer zu richten.

Der IT-SB ist bei allen Projekten, die deutliche Auswirkungen auf die Sicherheitsaspekte der Informationsverarbeitung haben, zu beteiligen.

Zu den Aufgaben des IT-SB gehören die Untersuchung IT-sicherheitsrelevanter Zwischenfälle und das Erstellen von Berichten zum Stand der IT-Sicherheit.

In seinen Aufgaben bezüglich der IT-Sicherheit ist der IT-SB nur an Weisungen der Hochschulleitung gebunden.

Die Universität hat sicherzustellen, dass der IT-SB für seine Aufgaben zur IT-Sicherheit im erforderlichen Umfang von seinen übrigen Aufgaben entlastet und angemessen ausgestattet wird.

(5) Leiter IT-Servicezentrum (L-ITS)

Der L-ITS ist verantwortlich für die IT-Sicherheit der vom IT-Servicezentrum betriebenen IT-Infrastruktur und dokumentiert die im ITS realisierten Sicherheitsmaßnahmen. Er ist ständiges Mitglied der PK IKT und des AK IT-Sicherheit. Er führt die Beschlüsse der Hochschulleitung aus.

(6) Verantwortliche für IT-Systeme

Verantwortliche für IT-Systeme sind innerhalb ihres Bereichs berechtigt, neben den hochschulweiten IT-Sicherheitsmaßnahmen, eigene weiterführende Maßnahmen zu treffen. Bei möglichen Auswirkungen auf die IT-Infrastruktur der Universität ist eine Koordination mit dem IT-Servicezentrum notwendig. Die eigenverantwortlich getroffenen Maßnahmen sind zu dokumentieren.

§5 Gefahrenintervention

Das IT-Servicezentrum ist berechtigt, bei Gefahr im Verzug unmittelbar notwendige Abwehrmaßnahmen vorzunehmen. Bei den zu treffenden Maßnahmen ist der Grundsatz der Verhältnismäßigkeit der Mittel zu wahren. Die Maßnahmen sollten so erfolgen, dass der betroffene Nutzer - wenn irgend möglich - bereits vorher in Kenntnis gesetzt wird. Der betroffene Nutzer, die Leitung der betroffenen Einrichtung und der IT-SB sind unverzüglich über den Vorfall und die getroffenen Maßnahmen zu informieren.

Im Falle eines Vorfalls, der von einem Verantwortlichen für ein IT-System als potentiell IT-sicherheitsgefährdendes Ereignis eingestuft wird, ist dieser verpflichtet, geeignete Abwehrmaßnahmen zu treffen und das IT-Servicezentrum und den IT-SB von dem Ereignis und den getroffenen Maßnahmen schnellstmöglich in Kenntnis zu setzen.

Die Aufhebung der Gefahrenabwehrmaßnahmen erfolgt nach Durchführung hinreichender IT-Sicherheitsmaßnahmen.

§6 Vorbeugende Maßnahmen

Für die Sicherstellung der IT-Sicherheit sind vorbeugende Maßnahmen notwendig. Mit geeigneten technischen und organisatorischen Maßnahmen sollen Gefährdungsrisiken erfasst und eingedämmt sowie Angriffe auf die IT-Sicherheit frühzeitig erkannt werden. Bereichsübergreifende Maßnahmen werden im Arbeitskreis IT-Sicherheit koordiniert. Der Arbeitskreis IT-Sicherheit kann vorbeugende Maßnahmen vorschlagen. Die Durchführung vorbeugender Maßnahmen obliegt dem jeweils zuständigen IT-Systembetreiber.

§7 Finanzierung

Die personellen und finanziellen Ressourcen der zentralen IT-Sicherheitsmaßnahmen werden aus zentralen Mitteln der Hochschule finanziert.

Dem IT-SB wird aus zentralen Mitteln ein Etat für Fortbildungs-und Schulungskosten eingerichtet.

Weiterführende IT-Sicherheitsmaßnahmen finanziert der Teilbereich, der diese Maßnahmen initiiert und verantwortet.

§8 Aktualisierungsbestimmungen zur Aufrechterhaltung und Weiterentwicklung des IT-Sicherheitsprozesses

Der Arbeitskreis IT-Sicherheit hat die Aufgabe, die IT-Sicherheitsstrategie und die Wirksamkeit der bisherigen Organisationsform, Maßnahmen und Prozesse für IT-Sicherheit kontinuierlich zu überprüfen und weiterzuentwickeln und mindestens alle zwei Jahre darüber zu berichten.

§9 Inkrafttreten

Diese IT-Sicherheitsleitlinie für die Universität Bayreuth tritt am Tag der Veröffentlichung in Kraft.

Die vorliegende IT-Sicherheitsleitlinie wurde in der Sitzung der Hochschulleitung am 22.09.2015 beschlossen und am 17.05.2016 durch den Kanzler, Dr. Markus Zanner, veröffentlicht.