Informationssicherheitsleitlinie der Universität Bayreuth

Präambel

Für die Universität Bayreuth ist die Informations- und Kommunikationstechnik von zentraler Bedeutung zur 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.

Ziel ist es, Informationen und Daten sind in einer angemessenen Art und Weise so zu schützen, dass

(1) ihre Vertraulichkeit in angemessener Weise gewahrt ist und die Kenntnisnahme nur durch berechtigte Personen erfolgen kann,
(2) ihre Integrität durch ihre Richtigkeit und Vollständigkeit sichergestellt ist,
(3) ihre Verfügbarkeit gewährleistet ist, damit sie von den autorisierten Personen zum gewünschten Zeitpunkt in Anspruch genommen werden können,
(4) gesetzliche Verpflichtungen erfüllt werden können.

Die Informationssicherheitsleitlinie ergänzt die „Ordnung für die Informationsverarbeitungs-Infrastruktur der Universität Bayreuth“ in ihrer jeweils gültigen Fassung.

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

§1 Gegenstand der Informationssicherheitsleitlinie und Begriffsbestimmungen

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

Im Sinne dieser Leitlinie ist

1. "Informationssicherheit“:
   Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der informationsverarbeitenden und -lagernden technischen und nicht-technischen Systeme.
2. "IT-Infrastruktur":
   Gesamtheit der Hardware, Anwendungen und baulichen Einrichtungen der Universität, die der Informationsverarbeitung dienen.

3. "IT-System":
   Die funktionelle Einheit aus Hard-und Software, die Daten erhebt, erfasst, aufbereitet, nutzt, speichert, übermittelt, programmgesteuert verarbeitet, intern darstellt, ausgibt und wiedergewinnt.
4. „Informationssicherheitsprozess“:
   Die Gesamtheit der Verfahren, die das Ziel haben, Informationssicherheit in alle Abläufe der Universität zu integrieren, um eine konstante Weiterentwicklung und Verbesserung der Informationssicherheit zu gewährleisten.

§2 Geltungsbereich

Die Informationssicherheitsleitlinie 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 Informationssicherheit hinzuwirken und die dazu erforderlichen Maßnahmen zu treffen.
(2) Die Verantwortlichkeit für Informationssicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme.
(3) Alle Nutzer haben die Pflicht, Ereignisse, die die Informationssicherheit beeinträchtigen oder beeinträchtigen könnten, unverzüglich nach Kenntniserlangung dem IT-Servicezentrum zu melden. Das IT-Servicezentrum setzt anschließend den Informationssicherheitsbeauftragten (ISB) in Kenntnis.

§4 Beteiligte am Informationssicherheitsprozess und deren Aufgaben

(1) Hochschulleitung

Die Gesamtverantwortung für die Gewährleistung der Informationssicherheit und die Einhaltung des Informationssicherheitsprozesses 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 Informationssicherheit nach Rücksprache mit dem Informationssicherheitsbeauftragten (ISB) wahr.

(2) Präsidialkommission Informations- und Kommunikationstechnologie (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 Informationssicherheit werden der PK IKT berichtet. Nach Beschluss werden diese gegebenenfalls zur Genehmigung bzw. Inkraftsetzung an die Hochschulleitung weitergeleitet.

(3) Arbeitskreis Informationssicherheit (AK Informationssicherheit)

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

(4) Informationssicherheitsbeauftragter (ISB)

Der ISB wird von der Hochschulleitung ernannt. Der ISB ist ständiges Mitglied der PK IKT und des AK Informationssicherheit.

Der ISB hat ein Informations- und Vorschlagsrecht.

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

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

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

Zu den Aufgaben des ISB gehören die Untersuchung Informationssicherheitsrelevanter Zwischenfälle und das Erstellen von Berichten zum Stand der Informationssicherheit.

In seinen Aufgaben bezüglich der Informationssicherheit ist der ISB nur an Weisungen der Hochschulleitung gebunden.

Die Universität hat sicherzustellen, dass der ISB für seine Aufgaben zur Informationssicherheit in erforderlichem Umfang von seinen übrigen Aufgaben entlastet und angemessen ausgestattet wird.

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

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

(6) Verantwortliche für IT-Systeme

Verantwortliche für IT-Systeme sind innerhalb ihres Bereichs berechtigt neben den hochschulweiten Informationssicherheitsmaßnahmen 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 hat das Recht, 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 ISB 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 Informationssicherheitsgefährdendes Ereignis eingestuft wird, ist dieser verpflichtet, geeignete Abwehrmaßnahmen zu treffen und das IT-Servicezentrum und den ISB von dem Ereignis und den getroffenen Maßnahmen schnellstmöglich in Kenntnis zu setzen.

Die Aufhebung der Gefahrenabwehrmaßnahmen erfolgt nach Durchführung hinreichender Informationssicherheitsmaßnahmen.

§6 Vorbeugende Maßnahmen

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

§7 Finanzierung

Die personellen und finanziellen Ressourcen der zentralen Informationssicherheitsmaßnahmen werden aus zentralen Mitteln der Hochschule finanziert.

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

Weiterführende Informationssicherheitsmaßnahmen finanziert der Teilbereich, der diese Maßnahmen initiiert und verantwortet.

§8 Aktualisierungsbestimmungen zur Aufrechterhaltung und Weiterentwicklung des Informationssicherheitsprozesses

Der AK Informationssicherheit hat die Aufgabe, die Informationssicherheitsstrategie und die Wirksamkeit der bisherigen Organisationsform, Maßnahmen und Prozesse für Informationssicherheit kontinuierlich zu überprüfen und weiterzuentwickeln und mindestens alle zwei Jahre darüber zu berichten.

§9 Inkrafttreten

Diese Informationssicherheitsleitlinie für die Universität Bayreuth tritt am Tag der Veröffentlichung in Kraft.

Die vorliegende Informationssicherheitsleitlinie wurde in der Sitzung der Hochschulleitung am 24.09.2019 beschlossen. Sie tritt an Stelle der IT-Sicherheitslinie, die in der Sitzung der Hochschulleitung am 22.09.2015 verabschiedet wurde.