Leitlinie zur Informationssicherheit der Hochschule Furtwangen

Vorwort

Die Leistungsfähigkeit der Hochschule Furtwangen in den Bereichen Forschung, Lehre und Verwaltung hängt maßgeblich von der Sicherheit und Verfügbarkeit der erforderlichen Informationen ab. Aufgrund der steigenden Anzahl innerer und äußerer Angriffe auf die IT-Infrastruktur hat das Ergreifen von Maßnahmen zur Sicherung der Infrastruktur höchste Priorität.

Dieses Dokument beschreibt den Informationssicherheitsprozess der Hochschule Furtwangen und dient als Grundlage für ein Informationssicherheitskonzept. Die daraus resultierenden Prozesse und Maßnahmen sollen eine größtmögliche Sicherheit im Bereich der Informationstechnik gewährleisten. Besondere Aufmerksamkeit gilt dem Schutz der Verarbeitung personenbezogener Daten.

Voraussetzung für ein gut funktionierendes Informationssicherheitsmanagement ist eine klare Organisation der Verantwortungsstrukturen in der Hochschule Furtwangen. Grundlage für die Implementierung geeigneter IT-Schutzmaßnahmen ist außerdem die regelmäßige Durchführung von Risikobewertungen der IT-Dienstleistungen hinsichtlich der Verletzung von Schutzzielen.

Geltungsbereich

Diese Leitlinie gilt für alle Einrichtungen der Hochschule Furtwangen, die gesamte IT-Infrastruktur einschließlich der von den Fakultäten betriebenen IT-Systeme, der zentralen Einrichtungen sowie alle am HFU-Netz angeschlossenen Geräte und alle Mitglieder, Angehörige und Gäste der Hochschule Furtwangen.

Ziele

Die primären Ziele der Informationssicherheit sind

- *Verfügbarkeit*: die Nutz- und Erreichbarkeit aller für die Aufrechterhaltung des Betriebs erforderlichen Informationen und der zugehörigen IT-gestützten Dienste, Daten und der IT-Infrastruktur zu gewährleisten.
- *Vertraulichkeit*: Daten und IT-Diensten vor unbefugtem Zugriff zu schützen.
- *Integrität:* Integrität von Daten und IT-Diensten zu garantieren, d.h. vor unbefugten Änderungen zu schützen.

– *Wahrung gesetzlicher Vorgaben:* Vorgaben zur Speicherung und Verarbeitung personenbezogener Daten einzuhalten.

Diese Ziele und dementsprechend die Maßnahmen zum Erreichen der Ziele orientieren sich an den Vorgaben des IT-Grundschutzes des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dabei gilt dem Datenschutz besondere Aufmerksamkeit. Neben den erwähnten Primärzielen sollen zusätzlich auch:

- die IT-Systeme/IT-Infrastruktur vor innerem und äußerem Missbrauch geschützt werden.
- der reibungslose Ablauf in Forschung, Lehre und Verwaltung gewährleistet werden.
- der gute Ruf der Hochschule Furtwangen in der Öffentlichkeit gewahrt werden.

Organisation

Die folgenden Akteure und Organisationseinheiten haben im Informationssicherheitsmanagement (Information Security Management System, ISMS) eine tragende Rolle:

Rektorin oder Rektor

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Rektorin oder beim Rektor der Hochschule Furtwangen.

Informationssicherheitsbeauftragte/r (Chief Information Security Officer, CISO)

Die oder der Informationssicherheitsbeauftragte wird vom Rektorat der Hochschule Furtwangen benannt und ist für die Planung, Koordination und Umsetzung der Maßnahmen zur Gewährleistung der Schutzziele zuständig. Zu ihren oder seinen Aufgaben gehört unter anderem die regelmäßige Risikoevaluierung der zu schützenden Systeme und Dienste.

Datenschutzbeauftragte/r

Die oder der Datenschutzbeauftragte wird vom Rektorat der Hochschule Furtwangen benannt. Sie oder er unterstützt das Rektorat dabei, die Verarbeitung personenbezogener Daten unter Einhaltung der EU-Datenschutzgrundverordnung (DS-GVO), des LDSG bzw. BDSG (sofern anwendbar) sowie anderer gesetzlicher Regelungen durchzuführen.

Dies umfasst unter anderem die Einhaltung der Meldepflicht von sicherheitsrelevanten Vorfällen bei der Verarbeitung von personenbezogenen Daten sowie die Überprüfung, ob mögliche Informationssicherheitsmaßnahmen der EU-Datenschutzgrundverordnung bzw. dem LDSG zuwiderhandeln.

Gemäß der Vorgaben der DS-GVO trägt die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt. Die oder der Datenschutzbeauftragte unterliegt bei Anwendung seiner Fachkunde nicht den Weisungen des Rektorats.

Die Amtszeit der oder des Datenschutzbeauftragten beträgt vier Jahre und beginnt jeweils am ersten März. Eine erneute Bestellung ist möglich.

Personalrat

Der Personalrat vertritt die Interessen der Mitarbeiterinnen und Mitarbeiter. Er muss zudem möglichen Dienstvereinbarungen zustimmen.

Stabsstelle für Informationssicherheit und Datenschutz

Die Mitarbeiterin oder der Mitarbeiter der Stabsstelle für Informationssicherheit und Datenschutz ist für die Durchführung des Informationssicherheitsprozesses verantwortlich und unterstützt hierdurch die oder den Datenschutzbeauftragen sowie die oder den Informationssicherheitsbeauftragten. Zu den weiteren Aufgaben gehören unter anderem die Konzeption und Durchführung von Schulungen der Mitarbeiterinnen und Mitarbeiter, die Erstellung der relevanten Dokumente (u.a. Verfahrensverzeichnis) und die Abwicklung der Sitzungen des Informationssicherheitsmanagement-Teams.

Informationssicherheitsmanagement-Team

Das Informationssicherheitsmanagement-Team (ISMT) berät und unterstützt zum einen die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten bei der Umsetzung und Steuerung des Informationssicherheitsprozesses und zum anderen die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Einschätzung schwerwiegender Datenschutzverletzungen. Außerdem werden die Schutzbedarfe der IT-Systeme ermittelt, welche sich durch sich ändernde Gefährdungseinschätzungen der IT-Systeme ergeben.

Das Informationssicherheitsmanagement-Team besteht aus:

- Rektorin oder Rektor bzw. ihre oder seine Stellvertreterin oder Stellvertreter
- Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter
- Datenschutzbeauftragte oder Datenschutzbeauftragter
- Vertreterin oder Vertreter des Personalrats
- Stabsstelle für Informationssicherheit und Datenschutz

Umsetzung des Informationssicherheitsprozesses

Vorgehen im Informationssicherheitsprozesses

Grundlage des Informationssicherheitsprozesses ist eine Strukturanalyse zur Ermittlung des Schutzbedarfes der einzelnen IT-Systeme und -Anwendungen, um einen Basisschutz zu definieren. Daraus wird für die Hochschule Furtwangen entsprechend den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein allgemeines Informationssicherheitskonzept erstellt.

Folgende Prinzipien sollten bei der Erstellung eines einheitlichen Konzeptes berücksichtigt werden:

- Sensibilisierung der HFU-Mitglieder bezüglich der Informationssicherheit
- IT-Systeme und Daten werden dem Stand der Technik entsprechend vor unberechtigten Zugriffen geschützt,
- Datensicherungen werden durchgeführt, um Benutzerfehlern oder technischem Versagen vorzubeugen,
- IT-Systeme werden in einer sicheren Umgebung betrieben,
- IT-Systeme werden auf dem aktuellen Stand gehalten,

- IT-Systeme werden adäquat vor schädlicher Software (sog. Malware) geschützt,
- die Sicherheitsmaßnahmen werden regelmäßig auf ihre Wirksamkeit hin überprüft und dokumentiert sowie dem Stand der Technik entsprechend angepasst sowie
- IT-Sicherheitsvorfälle werden dokumentiert und kommuniziert.

Aufbauend auf dieser Leitlinie werden in enger Anlehnung an ISO 27001 sowie IT Infrastructure Library (ITIL) allgemeine und detaillierte Richtlinien erarbeitet, in denen sowohl dienste-spezifische als auch zielgruppenbezogene Maßnahmen beschrieben werden.

Verbesserung der Sicherheit

Das Gesamtkonzept der Informationssicherheit wird regelmäßig auf seine Aktualität, Angemessenheit und Wirksamkeit geprüft. Das Rektorat unterstützt die ständige Verbesserung des Sicherheitsniveaus. HFU-Mitarbeiterinnen und Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben. Durch eine kontinuierliche Revision der Regelungen bzw. Richtlinien und deren Einhaltung wird das angestrebte Sicherheitsniveau gefestigt. Abweichungen werden mit dem Ziel analysiert, das IT-Sicherheitsniveau zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

Inkrafttreten

Diese Richtlinie tritt am 01.02.2018 in Kraft.

Furtwangen, 29.01.2018

gez. Prof. Dr. Rolf Schofer

Rektor