Fachhochschule
Dortmund
University of Applied Sciences and Arts

we
focus
on
students

IT-Sicherheitsleitlinie der Fachhochschule Dortmund

vom 02. Oktober 2019

IT-Sicherheitsleitlinie
der Fachhochschule Dortmund

vom 02. 10 .2019

Das Rektorat der Fachhochschule Dortmund hat die folgende IT-Sicherheitsleitlinie als interne Richtlinie mit Beschluss vom 02. Oktober 2019 erlassen.

§ 1 Geltungsbereich

Die vorliegende Leitlinie bildet die Basis für die IT-Sicherheit und die hierfür erforderlichen Sicherheitsrichtlinien und Maßnahmen. Zum Schutz der Informationstechnologie (IT) und der Datenverarbeitung der Fachhochschule Dortmund sind die Sicherheitsleitlinie und die daraus abgeleiteten Richtlinien und Maßnahmen für alle Angehörigen und Mitglieder der Fachhochschule verbindlich.

Eine Hochschule ist nur arbeitsfähig, wenn ihre Mitglieder einen möglichst fehlerlosen Zugriff auf die IT als wesentlicher Basis aller Arbeitsabläufe haben. Alle Mitglieder und Angehörige der Fachhochschule sind von der Verfügbarkeit der IT abhängig. Absehbare Schäden und Gefahren für die Hochschule müssen abgewehrt werden, um einen reibungslosen Ablauf des Hochschulbetriebes sicherzustellen. Neben der Sicherstellung von Abläufen muss die Einhaltung rechtlicher Verpflichtungen, z.B. des Datenschutzes, hochschulweit gewährleistet sein. Eine funktionierende Sicherheits-Governance soll die Verfügbarkeit, die Integrität und Vertraulichkeit der Datenverarbeitung gewährleisten.

§ 2 Sicherheits-Governance der Fachhochschule Dortmund

(1) Sicherheits-Governance bedeutet, durch Regeln, Organisation, Verfahrensweisen und deren Umsetzung einen geeigneten Sicherheitsstandard zu erreichen, der Gefährdungen und Schäden an der Hochschul-IT vorbeugt und einen Ausgleich zwischen einer möglichst großen Transparenz der genutzten Infrastruktur und notwendiger Schutzmaßnahmen findet.
Regeln, Organisation, Verfahrensweisen und Umsetzung einer Sicherheits-Governance richten sich nach den Gegebenheiten der Fachhochschule Dortmund.

(2) Die Sicherheits-Governance der Fachhochschule Dortmund soll durch folgende Punkte umgesetzt werden:

a) IT-Sicherheitsleitlinie

Auf oberster Ebene der Sicherheits-Governance definiert diese IT-Sicherheitsleitlinie grundlegende Ziele der Datensicherheit. Die Leitlinie legt Verantwortlichkeiten sowie Ziele fest und definiert Rahmenbedingungen für ihre Umsetzung.

b) IT- Sicherheitskonzept

Zur Erreichung der angestrebten Sicherheit sind der Schutzbedarf einzelner IT-Komponenten (unter anderem Infrastrukturkomponenten, Applikationen, Systeme, Webservices und Apps) und einzelner IT-Bereiche abzuschätzen und hierfür Sicherheitsrichtlinien aufzustellen. Dabei orientiert sich die Fachhochschule Dortmund grundsätzlich an den Empfehlungen des Bundesamtes für Sicherheit in der Informa-

tionstechnik (BSI) zur Erstellung von Sicherheitskonzepten. Diese beinhalten folgende Punkte:

1. Feststellung des Schutzbedarfs auf Grundlage der dokumentierten IT- und Prozesslandschaft,
2. Durchführung einer Risikoanalyse und
3. Festlegung von Sicherheitsstandards und Schutzmaßnahmen.

Im ersten Schritt erfolgt eine Zuordnung der IT-Komponenten in eine der folgenden Schutzbedarfskategorien (vergleichbar zum BSI- Standard).

- **Schutzbedarf „Niedrig bis Mittel“** (nach BSI: Normal)
  Schäden haben Beeinträchtigungen der Institution zur Folge.
- **Schutzbedarf „Hoch“**
  Im Schadensfall tritt Handlungsunfähigkeit zentraler Bereiche der Institution ein. Schäden haben erhebliche Beeinträchtigungen der Institution selbst oder betroffener Dritter zur Folge.
- **Schutzbedarf „Sehr hoch“**
  Der Ausfall der IT führt zum totalen Zusammenbruch der Institution oder hat schwerwiegende Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche.

Um den Schutzbedarf zu ermitteln, wird jede IT-Komponente auf den Verlust der Vertraulichkeit, Integrität und Verfügbarkeit geprüft.

c) IT- Sicherheitsrichtlinien

Die IT-Sicherheitsrichtlinien sind das Regelwerk, das anhand der im Sicherheitskonzept definierten Sicherheitsstandards Richtlinien und Regeln formuliert und Möglichkeiten der Realisierung aufzeigt.

Es sind proaktive und reaktive IT-Sicherheitsrichtlinien zu unterscheiden. Proaktive Sicherheitsrichtlinien dienen der Erreichung und Überwachung der angestrebten IT-Sicherheitsstandards. Reaktive Richtlinien sind Vorgaben für die Bearbeitung sicherheitsrelevanter Vorgänge.

Die AG IT-Sicherheit stellt eine Liste der durch sie verabschiedeten IT-Sicherheitsrichtlinien bereit und aktualisiert diese nach Erforderlichkeit. IT-Sicherheitsrichtlinien werden auf der Webseite der Hochschul-IT zur Einsicht für die Nutzer bereitgestellt. Die Fachbereiche und zentralen Einrichtungen weisen hierauf auf ihren Webseiten hin.

§ 3 Leitlinien des IT-Governance

Die IT-Sicherheits-Governance der Fachhochschule Dortmund basiert auf folgenden Grundsatzaussagen:

(1) Die Fachhochschule Dortmund ist bestrebt, einen offenen Informationsaustausch zu gewährleisten, sofern keine dienst-, urheber- oder datenschutzrechtlichen Belange verletzt werden.

(2) Die Durchsetzung, Aufrechterhaltung und dauerhafte Fortentwicklung der Sicherheitsstandards wird durch die Tatsache gewährleistet, dass die Hochschulleitung den Si-

cherheitsprozess über die AG IT-Sicherheit initiiert und aktiv unterstützt. Ein rein auf Fachbereichs- bzw. Einrichtungsebene initiierter Sicherheitsprozess kann keine dauerhafte Fortentwicklung der angestrebten Sicherheitsstandards gewährleisten.

(3) Sicherheit kann nur erreicht werden, wenn hochschulweit gültige Sicherheitsstandards definiert werden und diese ggf. gestuft auf der Ebene von Fachbereichen, Zentralen Einrichtungen und der Verwaltung erfolgreich umgesetzt werden.

(4) Sicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzerinnen und Nutzern der IT wahrgenommen werden muss. Sie kann nur erfolgreich umgesetzt werden, wenn die Nutzerinnen bzw. Nutzer für Belange der Sicherheit sensibilisiert und über das Gefährdungspotential und mögliche Gegenmaßnahmen in ihrem Arbeitsumfeld informiert werden.

(5) Sicherheit ist kein Selbstzweck. Sie muss daher stets die Verhältnismäßigkeit der Maßnahmen und Mittel im Spannungsfeld zwischen Informationsoffenheit, Kosten und Nutzerakzeptanz auf der einen und dem notwendigen Grad von Sicherheit auf der anderen Seite berücksichtigen.

(6) Der Schutz der in der IT gehaltenen und verarbeiteten Daten gegen absichtliches Löschen, Verfälschen oder auch unabsichtlichen Verlust ist durch angemessene Maßnahmen der Datensicherung zu gewährleisten.

(7) Die IT-Sicherheitsrichtlinien sind permanent weiter zu entwickeln und zu ergänzen, um zeitnah neue Risiken festzustellen und geeignete Gegenmaßnahmen zu identifizieren.

§ 4 IT-Sicherheitsziele

Die an der Fachhochschule Dortmund angestrebten Sicherheitsstandards dienen dem Schutz der in der IT der Fachhochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen, insbesondere im Hinblick auf:

a) Zugänglichkeit/Verfügbarkeit

Daten und Anwendungen müssen dem jeweiligen Nutzungsprofil entsprechend jederzeit von jedem Arbeitsplatz bei Bedarf verfügbar sein. Voraussetzung für die Aufrechterhaltung der Datenverfügbarkeit ist die Sicherung aller IT-Komponenten und der technischen und räumlichen Infrastruktur gegen organisationsbedingte, technische und umweltbedingte Ausfälle. Zentrale, aber auch dezentrale IT-Systeme müssen funktionieren, um die Verfügbarkeit der Daten zu garantieren. Zudem müssen Daten regelmäßig gesichert werden.

b) Integrität

Daten und Anwendungen dürfen nicht unberechtigt gelöscht, zerstört oder manipuliert werden können.

c) Vertraulichkeit

Daten und Anwendungen dürfen grundsätzlich nur von Personen gelesen und benutzt werden, die dazu eine Zugriffsberechtigung besitzen. Die Festlegung der Zugriffsberechtigung und des erforderlichen Kontrollumfangs obliegt der einsetzenden Stelle. Wegen der Gestaltung und der Auswahl von Verfahren zur Verarbeitung personenbezogener Daten ist die bzw. der behördliche Datenschutzbeauftragte rechtzeitig einzubinden. Gleiches gilt für die Neueinführung und Änderung der entsprechenden Verfahren.

§ 5 Arbeitsgruppe IT-Sicherheit

(1) Die AG IT-Sicherheit ist das zentrale Gremium zur Umsetzung der IT-Sicherheitsleitlinie, zur Erstellung des IT-Sicherheitskonzeptes und der IT-Sicherheitsrichtlinien.

(2) Um das Sicherheitskonzept und die Richtlinien hochschulweit umzusetzen und die angestrebten Sicherheitsstandards zu realisieren, sind entsprechende verbindliche Regelungen notwendig. Grundsätzlich wird angestrebt, vor allem durch Beratung und in Kooperation der Arbeitsgruppe mit den jeweiligen Organisationseinheiten die erforderlichen Sicherheitsstandards zu erreichen. Die AG IT-Sicherheit führt dabei folgende Maßnahmen durch:

a) Definition von zu bearbeitenden IT- Komponenten

   Die AG IT-Sicherheit legt jeweils pro Jahr Prozesse oder Bereiche fest, für die Risikoanalysen durchgeführt werden. Vorrangig sollen risikobehaftete Komponenten bearbeitet werden. Die AG IT-Sicherheit bestimmt die Maßstäbe zur Risikoeinschätzung, wobei sie sich nach den anerkannten Verfahren richtet, insbesondere den BSI Standards.

b) Prozessverantwortliche (Fachverantwortliche) und IT-Systemverantwortliche (Admins) sind von der AG IT-Sicherheit einzubeziehen. Die Verantwortlichen sind für eine Evaluation zur Risikoeinschätzung anhand der Vorgaben der AG IT-Sicherheit zuständig. Es soll eine möglichst vollständige Übersicht über die konkreten Prozesse und Risiken mit Einstufung in eine Schutzbedarfskategorie für die AG IT-Sicherheit erstellt werden. Die Verantwortlichen erläutern die Ergebnisse in der AG IT-Sicherheit und schlagen Sicherheitsmaßnahmen vor, die später in die IT-Sicherheitsrichtlinien eingehen sollen.

c) Die AG IT-Sicherheit überprüft die Vorschläge der Verantwortlichen nach b) und verabschiedet je Komponente eine konkrete Sicherheitsrichtlinie, in der das Risiko und die Schutzbedarfskategorie definiert und erforderliche technische und organisatorisch Schutzmaßnahmen, ggf. Fristen und Intervalle zur Überprüfung aufgelistet werden. Vor Verabschiedung wird den Leitern (Dekanen, Dezernenten, etc.) und IT-Sicherheitsbeauftragten der Einrichtungen die Möglichkeit zur Stellungnahme eingeräumt, sie können bei Bedarf auch schon vorher in den Prozess einbezogen werden.

d) Die Verantwortung für die Umsetzung der IT-Sicherheitsrichtlinie liegt bei den Prozessverantwortlichen nach b).

(3) Der AG IT-Sicherheit gehören an:

- LeiterIn der AG (vom Rektorat bestellt),
- CIO,
- IT-Sicherheitsbeauftragte/ -r,
- Datenschutzbeauftragte/ -r,
- die Fachbereiche, zentralen Einrichtungen und die Verwaltung benennen je eine Person als Vertretung und
- je ein/-e Vertreter/ -in der Personalräte.

Die Personen können sich vertreten lassen.

Die AG trifft sich in der Regel einmal pro Semester sowie nach Bedarf. Maßnahmen werden mit Mehrheit der Stimmen der Mitglieder beschlossen. Auf Wunsch werden Ergebnisse dem Rektorat sowie den Fachbereichs- und Einrichtungsleitungen berichtet.

Werden Vorgaben der AG nicht umgesetzt, kann dies an die/ den direkten Vorgesetzten und ggf. an Rektor/ -in und/ oder Kanzler/ -in mitgeteilt werden. Diese können Weisungen erteilen.

Ausgefertigt aufgrund des Beschlusses des Rektorats der Fachhochschule Dortmund vom 02.10.2019.

Dortmund, den 28.01.2020
Der Rektor

Prof. Dr. Wilhelm Schwick