



Modulhandbuch

Datenschutz und IT-Sicherheit (SPO WS 21/22)

Fakultät Wirtschaft

Wintersemester 2021/22

Stand: 14.12.2021



Inhalt

1	Vorstellung Studiengang	3
2	Modulbeschreibungen	5
2.1	Pflichtmodule.....	6
2.2	Praktisches Studiensemester.....	53
2.3	Bachelorarbeit	63
2.4	Spezialisierungen	68
2.5	Vertiefung/Erweiterung der Spezialisierungen	83
2.6	Fachspezifisches Wahlpflichtmodul.....	88
2.7	Allgemeine Wahlpflichtmodule	97

1 Vorstellung Studiengang

STUDIENGANG			
Kurzform:	DIS	SPO-Nr.:	
Studiengangleitung:	Prof. Dr. Wolf Knüpffer		
Studienfachberatung:	Prof. Dr. Wolf Knüpffer		
ECTS:	210 Punkte		
Regelstudienzeit:	7 Semester		
Teilnahmevoraussetzung:	Hochschulreife (allgemeine oder fachgebundene), Fachhochschulreife, Hochschulzugang für (besonders) qualifizierte Berufstätige		
Verwendbarkeit:	Bachelor Datenschutz und IT-Sicherheit		
Angestrebte Lernergebnisse:			
Ziel des Studiums ist es, mit anwendungsbezogener Lehre auf wissenschaftlicher Grundlage Datenschutz- und IT-Sicherheitsexperten/-innen mit Beschäftigungs- und Arbeitsmarktbefähigung und der Qualifikation für Master-Studiengänge auszubilden. Das Studium befähigt die Absolventen/-innen dazu, interdisziplinäre Zusammenhänge im Kontext Datenschutz zu verstehen, diese zu analysieren, organisatorisch und rechtlich abzusichern sowie technische Sicherheitslücken in der IT-Infrastruktur zu identifizieren und zu schließen. Im Mittelpunkt des Studiums steht die anwendungsorientierte, wissenschaftlich fundierte Vorbereitung der Studierenden auf berufliches Handeln. Im Hinblick auf die verschiedenen Einsatzmöglichkeiten der Datenschutz- und IT-Sicherheitsexperten/-innen erreicht der Studiengang die Berufsbefähigung seiner Absolventen/-innen dabei durch Förderung in folgenden Kompetenzfeldern: - Fachkompetenzen im Sinne der Beherrschung grundlegender Konzepte und Methoden, die über aktuelle Trends hinaus Bestand haben und die es dem/der Hochschulabsolventen/-in erlauben, sich selbständig in neue Erscheinungsformen des Datenschutzes und der Informationstechnologie einzuarbeiten sowie Fachkompetenz im Sinne der Fähigkeit zu abstrahieren von den Anwendungskonventionen bestimmter Werkzeuge, hin zu den dahinterliegenden organisatorischen und rechtlichen Ansätzen und Informatikkonzepten. - Handlungskompetenz im Sinne einer Umsetzungsfähigkeit der erworbenen Kernkompetenzen im beruflichen Umfeld sowie praktische Problemlösungsfähigkeit auf der Grundlage des Methodenwissens. - Sozialkompetenz im Sinne persönlichkeitsorientierter Schlüsselqualifikationen, die es den Absolventen/-innen ermöglichen, ihre erworbenen Kern- und Handlungskompetenzen im betrieblichen Umfeld in Arbeitsgruppen, Projekten, Besprechungen und Präsentationen wirksam werden zu lassen. Hierzu zählt auch die Ausdrucksfähigkeit in einer Fremdsprache.			
Inhalt:			
Die Regelstudienzeit beträgt sieben Semester mit einem Gesamtvolumen von 210 ECTS- Punkten. Das Studium gliedert sich in sechs theoretische und ein praktisches Studiensemester. Der studentische Arbeitsaufwand beträgt 30 Stunden pro ECTS-Punkt.			

Das Studium ist in folgende Modulgruppen gegliedert:

- Pflichtmodule (PM)
- Allgemeine Wahlpflichtmodule (AWPM)
- Fachspezifische Wahlpflichtmodule (FWPM)
- Spezialisierungen (SPM)
- Vertiefung oder Erweiterung der Spezialisierungen (VESPM)
- Praktisches Studiensemester (PrS)
- Bachelorarbeit (BAr)

Zur berufsbezogenen Spezialisierung werden nach Maßgabe des Studienplans Spezialisierungsmodule angeboten. Es müssen zwei Spezialisierungen (SPM) mit jeweils zwei Modulen und zwei Module zur Vertiefung oder Erweiterung der Spezialisierungen (VESPM) gewählt werden.

Abschluss / Akademischer Grad:

Bachelor of Arts, Kurzform: „B.Sc.“

2 Modulbeschreibungen

2.1 Pflichtmodule

Einführung in die IT-Sicherheit			
Modulkürzel:	DIS-Einführung in die IT-Sicherheit	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	1	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	8 ECTS / 6 SWS		
Arbeitsaufwand:	Kontaktstunden:	68 h	
	Selbststudium:	172 h	
	Gesamtaufwand:	240 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Einführung in die IT-Sicherheit		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden verfügen über ein breites Grundlagenwissen im Bereich IT-Sicherheit, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Einsatzgebiete der IT-Sicherheit in einer Organisation und kennen die typischen Problemstellungen und Lösungsansätze der Informatik dafür. Darauf aufbauend verfügen die Studierenden über die Fähigkeit Entwicklungen und Tendenzen im Bereich der IT-Sicherheit kritisch zu hinterfragen und Querbeziehungen zu erkennen. Handlungskompetenz Die Studierenden können grundlegende fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von IT-Sicherheitswerkzeugen bzw. -Appliances, Methoden oder Konzepten aktiv mitwirken, um den operativen Betrieb einer Organisation möglichst sicher zu gestalten. Basierend auf der erworbenen Fachkompetenz können die Studierenden im 4. Fachsemester eine fundierte Wahl der Studienschwerpunkte treffen. Sozialkompetenz Aufbauend auf ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.			
Inhalt:			
• Motivation IT-Sicherheit: Aktuelle Fälle der IT-Sicherheit – Vorstellung, Recherche • Bedrohungsszenarien, grundlegende Angriffsvektoren, z.B.			

- o Social Engineering
- o Hacking
- o (Distributed) Denial of Service (DDOS)
- Erster Einstieg in die Kryptoanalyse:
 - o Brute-Force
 - o Wörterbuchangriff, Rainbow tables
 - o Man-in-the-Middle
- Grundbegriffe der IT-Sicherheit: Vertraulichkeit, Integrität, Authentizität, Nichtabstreitbarkeit, Zurechnbarkeit/Accountability, Access Control, etc.
- Standards in der IT-Sicherheit: IT-Sicherheitsmanagement, Grundschutzkatalog BSI, ISO 27001
- Biometrie, Authentifizierung, Zugriffs-/Zugangskontrolle
- Der Faktor Mensch in der IT-Sicherheit, Awareness IT-Sicherheit, Benutzbare Sicherheit
- Notfallplanung, Response, Veröffentlichung
- Ausblick / Motivation Datenschutz

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, 10th expanded and updated edition (21. August 2018), De Gruyter Verlag, ISBN: 978-3110551587
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487
- Tom DeMarco, Timothy R. Lister: „Wien wartet auf Dich! -Der Faktor Mensch im DV-Management“ (engl. „Peopleware“), 2. Auflage, Hanser Verlag, ISBN: 3-446-21277-9

Datenschutzrecht I			
Modulkürzel:	DIS-Datenschutzrecht I	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	1	
Modulverantwortliche(r):	Prof.Dr. Sascha Müller-Feuerstein		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Datenschutzrecht 1		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden verfügen über Grundlagenwissen im Bereich des Datenschutzrechts, welches sie u.a. zur Teilnahme an weiterführenden Lehrveranstaltungen befähigt. Die Studierenden besitzen ein grundlegendes Verständnis wichtiger Prinzipien und Konstituenten des Datenschutz- und IT-Rechts, kennen die typischen Fragestellungen im Kontext der EU-DSGVO und nachfolgender Rechtsvorschriften. Darauf aufbauend verfügen die Studierenden über die Fähigkeit Entwicklungen und Tendenzen im Bereich des Datenschutzrechts kritisch hinterfragen und Querbeziehungen erkennen zu können. Handlungskompetenz Die Studierenden können weitgehend eigenständig einfach Fragestellungen im Bereich des Datenschutzrechts beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage typische Fragestellungen in Organisationen als relevant für eine Datenschutzrechtliche Betrachtung zu erkennen. Sozialkompetenz Die Studierenden können die Prinzipien des modernen Datenschutzes allgemeinverständlich erklären und plausibel herleiten. Aufbauend darauf können Sie in einer Organisation für grundlegendes Verständnis und Awareness bzgl. der täglichen Umsetzung des Datenschutzes sorgen.			
Inhalt:			
• Rechtliche Grundlagen • Grundsätze des Datenschutzrechts • Rechte der Betroffenen • Verantwortliche und Auftragsverarbeiter • BDSG-neu & Erwägungsgründe			

- IT- und Computerrecht
- Typische/Beispielhafte Fragestellungen in der Praxis

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Ivo Geis, et al.: Datenschutzrecht, 11. Auflage (15. Oktober 2018), dtv Verlagsgesellschaft, ISBN: 978-3423057721
- Jürgen Kühling et al.: Datenschutzrecht (Start ins Rechtsgebiet), 4., völlig neu bearbeitete Auflage 2018 (28. März 2018), ISBN: 978-3811445710
- Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621
- Helmut Redeker: IT-Recht, 6. Auflage, neubearbeitete (28. November 2016), C.H.Beck Verlag, ISBN: 978-3406687273
- DSK-Kurzpapiere (<https://www.datenschutzkonferenz-online.de/kurzpapiere.html>)

Programmierung I			
Modulkürzel:	DIS-Programmierung I	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	1	
Modulverantwortliche(r):	Prof. Dr. Bernhard Volz		
Sprache:	Deutsch		
Leistungspunkte / SWS:	7 ECTS / 6 SWS		
Arbeitsaufwand:	Kontaktstunden:	68 h	
	Selbststudium:	142 h	
	Gesamtaufwand:	210 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Programmierung I		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden können einfache Programme in einer höheren Programmiersprache entwickeln und wenden dabei die Prinzipien der strukturierten Programmierung an. Sie verstehen es, geeignete Sprachelemente bei der Umsetzung von Programmierproblemen in lauffähige Programme zu verwenden. Handlungskompetenz Die Studierenden können einfache Programme (Konsolprogramme) für betriebliche Aufgabenstellungen entwerfen und implementieren.			
Inhalt:			
• Programmiersprachen allgemein (Arten, Konzepte) • Grundlegende Einführung in die Syntax und Semantik einer höheren Programmiersprache (elementare und komplexe Datentypen, Anweisungen, Kontrollstrukturen), Einsatz von Programmbibliotheken; • Einführung in die Grundlagen der objektorientierten Programmierung (Klassen, Objekte, Attribute, Methoden); • Entwicklungsmethodik für das Programmieren im Kleinen, schrittweise Verfeinerung, Prinzipien der strukturierten Programmierung; • Einführung in eine moderne Entwicklungsumgebung für das Erstellen, Verwalten und Testen von Programmen			

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten (elektronische Fernprüfung nach § 2 Abs. 1 BayFEV)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage
- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage
- Guido Krüger: Java-Programmierung – das Handbuch, O'Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage

Grundlagen der Informatik			
Modulkürzel:	DIS-Grundlagen der Informatik	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	1	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Grundlagen der Informatik		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	keine		
Empfohlene Voraussetzungen:	keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden haben einen umfassenden Überblick über die wichtigsten Aspekte moderner Betriebs- und Kommunikationssysteme. Sie kennen die Anforderungen an moderne Betriebssysteme und die Grundkonzepte für deren Lösung in verschiedenen Betriebssystemen. Sie haben das Prinzip der Abstraktion durch Definition von Netzwerkschichten verinnerlicht und können aktuelle Kommunikationstechnologien vor dem Hintergrund ihrer historischen Entwicklung einordnen und verstehen. Handlungskompetenz Die Studierenden können im Rahmen des Aufbaus von IT-Lösungen in einfachen Kommunikationsszenarien Empfehlungen für die Auswahl geeigneter Betriebssysteme und Kommunikationsmittel aussprechen. Aufgrund des erworbenen Grundwissens sind sie in der Lage, auch zukünftige Entwicklungen in diesen Bereichen einzuordnen und zu bewerten.			
Inhalt:			
Das Modul ist in zwei Teile gegliedert. Unter anderem werden folgende Themen behandelt: Teil I: Betriebssysteme: • Einführung in die Architektur moderner Betriebssysteme, • Methoden der Prozess- und Betriebsmittelsteuerung, • Methoden zur Hauptspeicherverwaltung, • Aufbau moderner Dateiverwaltungssysteme und Methoden der Dateiverwaltung.			

Teil II: Kommunikationssysteme:

- Darstellung wesentlicher Entwicklungen im Bereich der Kommunikationstechnik,
- Funktionen von Kommunikationssystemen, Netzwerktopologien und – technologien,
- Netzwerk-Protokolle, Netzwerk-Referenzmodellen (ISO/OSI, TCP/IP),
- Algorithmen und Strategien für das Routing, Netzlaststeuerung,
- Fehlerbehandlung, Zugriffssteuerung,
- Anwendungsprotokolle (HTTP, IMAP, POP3, FTP, etc.),
- Netzwerkgeräte (Hub, Bridge, Switch, Router, Gateway, etc.).

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

Übergreifende Literatur:

- Hansen, R., Neumann G.: Wirtschaftsinformatik 2; Informationstechnik. 9. Auflage, Lucius & Lucius, Stuttgart 2005.

Zu Teil I:

- Brause, R.: Betriebssysteme - Grundlagen und Konzepte. Springer-Verlag, Berlin-Heidelberg, 2. Auflage, 2013. ISBN 3540009000

- Stallings, W.: Betriebssysteme – Prinzipien und Umsetzung. Prentice Hall. 4. Auflage, 2003.

ISBN 3-8273-7030-2

- A.-S. Tanenbaum: Moderne Betriebssysteme. Addison-Wesley Longman, 4. Auflage, 2016.

ISBN 3-8273-70719-1

Zu Teil II:

- Andrew, S. Tanenbaum, David J. Wetherall: Computernetzwerke. Pearson
- James, F. Kurose, Keith W. Ross: Computernetzwerke: Der Top-Down-Ansatz. Pearson
- Schreiner, R.: Computernetzwerke, Von den Grundlagen zur Funktion und Anwendung. Hanser

Big Data Analytics und Statistik			
Modulkürzel:	DIS-Big Data Analytics und Statistik	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	1	
Modulverantwortliche(r):	Prof. Dr. Bernhard Volz		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Big Data Analytics und Statistik		
Lehrformen des Moduls:	2 SWS seminaristischer Unterricht Big Data Analytics, 2 SWS seminaristischer Unterricht Statistik		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Big Data Analytics Die Studierenden beherrschen Methoden, um mit großen Datenbeständen in der statistischen Programmiersprache R umzugehen. Dies deckt den kompletten Data Analysis Lifecycle ab: Daten laden, bereinigen und transformieren sowie modellieren. Ergänzt wird dies durch Vermittlung von Methoden zur Visualisierung und Kommunikation von Analyseergebnissen. Die Übungseinheiten thematisieren die einzelnen Themenbereiche und trainieren die praktische Umsetzung aller Schritte in der Programmiersprache R. Statistik Die Studierenden sollen die wichtigsten Grundkonzepte aus den Bereichen der deskriptiven und induktiven Statistik verstehen. Ergänzend werden Inhalte der Elementaren Wahrscheinlichkeitsrechnung als Basis vermittelt. Abschließend befasst sich der Kurs mit Indexrechnung. Neben der Vermittlung von theoretischem Verständnis zielt die Veranstaltung auf die konkrete Anwendung der kennengelernten Techniken im Zuge der Übungseinheiten ab. Fach- und Methodenkompetenz: Studierenden werden befähigt • die Anwendung statistischer Methoden zur Analyse und zur Interpretation von Daten zu verstehen, • Daten aufzubereiten und so darzustellen, dass diese zu bestimmte Inhalte objektiv vermitteln, • selbständig statistische Tests und Analysen durchzuführen sowie • die Sprache R für Datenimport, -aufbereitung sowie -auswertung und Präsentation zu verwenden. Handlungskompetenz: Studierende können			

- Daten für die Analyse aufbereiten (Import, Bereinigung und Transformation)
- Daten anhand von Modellen interpretieren
- Schlussfolgerungen auf Basis einfacher, statistischer Tests ableiten

Sozialkompetenz:

Studierende können

- Auf den jeweiligen Anwendungsfall basierend den richtigen statistischen Test auswählen um ein bestimmtes Ziel zu validieren oder zu widerlegen
- Daten mit Hilfe von Modellen objektiv beschreiben und diese visuell aufbereitet kommunizieren

Inhalt:

Big Data Analytics:

1. Data Analysis Lifecycle
2. Datenaufbereitung: ETL-Prozess (Extraktion, Transformation, Loading) für einfache und große Datenbestände
3. Datenvisualisierung
4. Modellierung: Daten mit mathematischen Modellen beschreiben
5. Kommunikation von Modellen und Ergebnissen

Statistik:

1. Elementare Wahrscheinlichkeitsrechnung: Mengenoperationen und der Wahrscheinlichkeitsbegriff, Kombinatorik, Bedingte Wahrscheinlichkeit, Stochastische Unabhängigkeit, Bernoulli-Experiment
2. Deskriptive Statistik: Empirische Verteilungen, Verteilungsparameter (Lagemaße, Streuungsmaße, Zusammenhangsmaße), Theoretische Verteilungen (Diskrete und stetige Verteilungen)
3. Induktive Statistik: Punktschätzung, Intervallschätzung, Hypothesen-Tests, Regressionen
4. Indexrechnung

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten (elektronische Fernprüfung nach § 2 Abs. 1 BayFEV)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

Statistik:

1. Sibbertsen P.; Lehne H.: Statistik – Einführung für Wirtschafts- und Sozialwissenschaftler, 2. Auflage, Springer Gabler
- Grabmeier J.; Hagl S.: Statistik – Grundwissen und Formeln, 2. Auflage, Haufe
- Grolemond, G.; Wickham, H.: R for Data Science, 1. Auflage, O'Reilly, 2016
- Sauer, S.: Moderne Datenanalyse mit R, Springer Gabler, 2019

Mathematik			
Modulkürzel:	DIS-Mathematik	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof. Dr. Christine Dauth		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Mathematik		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS/WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden beherrschen die mathematischen Grundlagen, die als Instrumentarium in den verschiedenen fachspezifischen Modulen benötigt werden. Handlungskompetenz Die Studierenden sind in der Lage, das Instrumentarium der Mathematik anzuwenden, um Problemstellungen im Umfeld der Ökonomie zu analysieren und zu lösen.			
Inhalt:			
Lineare Algebra Lineare Gleichungssysteme; Matrizen und Vektoren; Grundlagen der Linearen Optimierung. Analysis Differentialrechnung mit einer und mit mehreren unabhängigen Veränderlichen, d.h.: Diskussion der bei ökonomischen Anwendungen wichtigsten Funktionen, Extremwertbestimmung ohne und mit Nebenbedingungen; Integralrechnung samt deren ökonomischen Anwendungen. Finanzmathematik Zins-, Renten- und Tilgungsrechnung.			
Studien- / Prüfungsleistungen:			
Studienarbeit (außerhalb Prüfungszeitraum)			

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

1. Schwarze, Jochen: Mathematik für Wirtschaftswissenschaftler, 5 Bände, Verlag Neue Wirtschaftsbriefe (NWB)
2. Holland, Heinrich und Doris Holland: Mathematik im Betrieb, Gabler-Verlag
3. Tietze, Jürgen: Einführung in die angewandte Wirtschaftsmathematik, Vieweg-Verlag
4. Ohse, Dieter: Mathematik für Wirtschaftswissenschaftler, 2 Bände, Verlag Franz Vahlen
5. Rommelfanger, Heinrich: Mathematik für Wirtschaftswissenschaftler, 2 Bände, Spektrum Akademischer Verlag

Programmierung II			
Modulkürzel:	DIS-Programmieren II	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof. Dr. Bernhard Volz		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Programmierung II		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Programmierung I		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Vertiefung der Fähigkeiten, die in Programmieren I erworben wurden. Die Studierenden beherrschen die Grundlagen und Konzepte der objektorientierten Programmierung und können diese in mindestens einer objektorientierten Programmiersprache anwenden. Handlungskompetenz Die Studierenden können Programme (Konsolprogramme, grafisch-interaktive) für anspruchsvolle betriebliche Aufgabenstellungen entwerfen und implementieren.			
Inhalt:			
• Einführung in die „Paradigmen“ der objektorientierten Programmierung (assoziative Beziehungen, Vererbung, Aggregation, Schnittstellen) • Vertiefung in objektorientierte Programmiertechniken (Polymorphismus, Kommunikation zwischen den Objekten, einfache Design-Pattern, Model-View-Controller Konzept (MCV), typische Datenstrukturen, Benutzung von Klassenbibliotheken, grafische Benutzeroberflächen)			
Studien- / Prüfungsleistungen:			
schriftliche Prüfung, 90 Minuten (elektronische Fernprüfung nach § 2 Abs. 1 BayFEV) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.			

Literatur:

- H. Mössenböck: Sprechen Sie Java? dpunkt.verlag, jeweils neuste Auflage
- Ratz, Scheffler, Seese, Wiesenberger: Grundkurs Programmieren in Java, Hanser, jeweils neuste Auflage
- Fritz Jobst: Programmieren in Java, Hanser, jeweils neuste Auflage
- Guido Krüger: Java-Programmierung – das Handbuch, O'Reilly, jeweils neuste Auflage
- Christian Ullenboom: Java ist auch eine Insel, Galileo Computing, jeweils neuste Auflage
- Anton Epple: JavaFX 8, Grundlagen und fortgeschrittene Techniken, dpunkt.verlag, 2016
- E. Gamma, R. Helm, R. Johnson, J. Vlissides: Design Patterns: Elementenst of Reusable Objekt-Oriented Software, Addison-Wesley Professional Computing Series, neueste Auflage

Technische und organisatorische Datenschutz-Maßnahmen			
Modulkürzel:	DIS-Techn. und organ. Daten- schutz-Maßnahmen	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Technische und organisatorische Datenschutz-Maßnahmen		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzun- gen:	Module Datenschutzrecht I und Einführung in die IT-Sicherheit		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden haben einen umfassenden Überblick über die wichtigsten technische und organisatorische Datenschutzmaßnahmen. Sie kennen die gesetzliche Datenschutz-Anforderungen an die Verarbeitung per- sonenbezogener Daten und die Grundkonzepte, um die entsprechende Sicherheitsziele zu gewährleisten. Handlungskompetenz Die Studierenden können im Rahmen des Aufbaus von einem Datenschutzmaßnahmenkonzept in einer Or- ganisation Empfehlungen für die Auswahl geeigneter Maßnahmenpaketen aussprechen. Aufgrund des er- worbenen Grundwissens sind sie in der Lage, auch zukünftige Entwicklungen in diesen Bereichen einzuord- nen und zu bewerten. Sozialkompetenz Die Studierenden sollen sich in einfachen fachlichen Diskussionen über technische und organisatorische Da- tenschutzmaßnahmen aktiv beteiligen können. Zudem sollen die Studierenden bei der Auswahl einer geeig- neten Maßnahmenpaket eine fundierte fachliche Meinung vertreten können.			
Inhalt:			
- Abgrenzung technische vs. organisatorische Datenschutzmaßnahmen - Gesetzlicher Rahmen: Art. 32 DSGVO, Art. 64 BDSG - Datenschutz und Sicherheitsziele: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit			

- Überprüfung, Bewertung, und Evaluierung der Wirksamkeit der Maßnahmen
- Management:
 - Behandlung von Sicherheitsvorfällen
 - Hardware und Software-Management: Patch-Management, ...
 - Personal Management: MA-Schulungen, ...
- Datensicherung, Archivierung, Datenlöschung
- Verschlüsselung und Pseudonymisierung
- Infrastrukturelle Sicherheitsmaßnahmen:
 - Zutrittskontrolle
 - Klimakontrolle
 - Maßnahmen gegen Feuer, Wasser, Über- und Unterspannung
- IT-Systeme und Netze:
 - Berechtigungsmanagement / Need-to-know-Prinzip
 - Mobile Device Management / VPN
 - Firewall/Antivirus/Back-up
 - Webserver / Mail-Server

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- U. Schläger, J. C. Thode: Handbuch Datenschutz und IT-Sicherheit, 1. Auflage (2018), Erich Schmidt Verlag GmbH & Company, ISBN: ISBN 978-3503177271
- Peter Münch: Technisch-organisatorischer Datenschutz: - Leitfaden für Praktiker, 4. Auflage (27. April 2010), DATAKONTEXT Verlag, ISBN: 978-3895775864

Bayerisches Landesamt für Datenschutzaufsicht (Herausgeber), Thomas Kranig, Eugen Ehmann: Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket, 1. Auflage (17. November 2017), Verlag C.H.Beck, ISBN: 978-3406716621

Algorithmen und Datenstrukturen			
Modulkürzel:	DIS-Algorithmen u. Datenstr.	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof. Dr. Bernhard Volz		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Algorithmen und Datenstrukturen		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS/WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Grundlegende Datenstrukturen und die dazugehörigen Algorithmen kennen und verstehen. Einfache Algorithmen analysieren, beschreiben und auf Korrektheit prüfen können. Algorithmen hinsichtlich ihres Laufzeitverhaltens und sonstigen Ressourcenverbrauchs bewerten können. Die algorithmische Komplexität von Programmieraufgaben einschätzen können. Handlungskompetenz Die Studierenden sollen die wichtigsten, im wirtschaftlichen Umfeld verwendeten Datenstrukturen und Algorithmen kennen, um für vorgegebene Anwendungsfälle geeignete Datenstrukturen und Algorithmen finden, analysieren und bewerten zu können. Überführung von realen Problemstellungen in geeignete, algorithmische Lösungen. Sozialkompetenz Die Studierenden sollen sich in einfachen fachlichen Diskussionen über Algorithmen und Datenstrukturen aktiv beteiligen können und z.B. bei der Auswahl einer geeigneten Datenstruktur eine fundierte fachliche Meinung vertreten können. Zudem sollen die Studierenden in der Lage sein, grundlegende Funktionsweisen von einfachen Algorithmen allgemeinverständlich zu erklären.			
Inhalt:			
- Was sind Algorithmen und Eigenschaften von Algorithmen - Elementare/grundlegende Datenstrukturen			

- Abstrakte Datenstrukturen (Stack, Queue, Bäume, Heap, Hash, ...)
- Algorithmische Verfahren (Suche, Sortierung, Rekursion, dynamische Programmierung, ...)
- Bewertung von Algorithmen und Datenstrukturen bzgl. Korrektheit, Komplexität, Effizienz und Aufwand

Studien- / Prüfungsleistungen:

mündliche Prüfung, 20 Minuten (elektronische Fernprüfung nach § 2 Abs. 3 BayFEV)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- T.H.Cormen, C.E.Leiserson, R.L.Rivest, C.Stein: Algorithmen – Eine Einführung, 4. Aufl., 2013, De Gruyter Oldenbourg
- R. Sedgewick, K. Wayne: Algorithmen: Algorithmen und Datenstrukturen, 2014, Pearson Studium – IT, neueste Auflage
- G. Saake, K.-W. Sattler: Algorithmen und Datenstrukturen: Eine Einführung mit Java, 5. Aufl., 2013, dpunkt Verlag

Datenschutzrecht II			
Modulkürzel:	DIS-Datenschutzrecht 2	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof.Dr. Sascha Müller-Feuerstein		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Datenschutzrecht 2		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden verfügen über vertieftes Wissen im Bereich des Datenschutzrechts und angrenzender Rechtsfelder. Die Studierenden besitzen ein umfassendes Verständnis der wichtigsten Rechtsvorschriften und können Rechtsfragen den einzelnen Rechtsgebieten zuordnen. Die Studierenden sind selbstständig in der Lage weitergehende Recherchen im Kontext des Datenschutzrechts durchzuführen und können klar Gültigkeiten und Zuständigkeiten abgrenzen. Handlungskompetenz Die Studierenden können weitgehend eigenständig fortgeschrittene Fragestellungen im Bereich des Datenschutzrechts und angrenzender Rechtsgebiete beantworten, bzw. Antworten begründet herleiten. Sie sind weiterhin in der Lage für typische Fragestellungen in Organisationen zu erkennen wann weitergehendes juristisches Fachwissen notwendig ist, bzw. wann ggf. Aufsichtsbehörden einzuschalten sind. Sozialkompetenz Die Studierenden können auch im vertieften Fachgespräch unter KollegInnen folgen und aktiv daran teilnehmen. Aufbauend darauf können Sie in einer Organisation an rechtskonformen Regelungen für den Datenschutz mitarbeiten.			
Inhalt:			
Verhaltensregeln und Zertifizierung			

- Vertiefung Datenschutzrecht und angrenzende Rechtsgebiete wie z.B. Telemediengesetz, Telekommunikationsgesetz
 - Übermittlung in Drittländer
 - Aufgaben der Aufsichtsbehörden
- Sanktionen

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Ivo Geis, et al.: Datenschutzrecht, 11. Auflage (15. Oktober 2018), dtv Verlagsgesellschaft, ISBN: 978-3423057721
- Geppert et al.: Telemediarecht Telekommunikations- und Multimediarecht: Telekommunikationsgesetz. Rahmenrichtlinie. Telekommunikations-Überwachungsverordnung. Netzwerkdurchsuchungsgesetz, 11. Auflage (8. Dezember 2017), dtv Beck Texte, ISBN: 978-3423055987
- DSK-Kurzpapiere (<https://www.datenschutzkonferenz-online.de/kurzpapiere.html>)

Kryptographie			
Modulkürzel:	DIS-Kryptographie	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	2	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Kryptographie		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Modul Mathematik		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden kennen die Bedeutung der wichtigsten kryptographischen Verfahren und kennen ihre typischen Einsatzbereiche. Die Studierenden verstehen die grundlegenden Konzepte der wichtigsten Verschlüsselungs-, Hash- und Authentifizierungsverfahren und die typischen Angriffsvektoren / Schwächen dieser Verfahren. Handlungskompetenz Die Studierenden können die grundlegenden Prinzipien kryptographischer Verfahren auch in neuen Verfahren erkennen und diese grob klassifizieren. Die Studierenden verstehen die prinzipiellen Vorteile, aber auch die Risiken des unsachgemäßen Einsatzes von kryptographischen Verfahren. Die Studierenden sind in der Lage zu erkennen, wann vertiefte fachliche Expertise zu Rate gezogen werden sollte. Sozialkompetenz Die Studierenden können einfachen Fachgesprächen zu den behandelten Konzepten folgen und in Diskussionen mit anderen Studierenden aktiv teilnehmen. Die Studierenden können die grundlegenden Prinzipien der symmetrischen und asymmetrischen Verschlüsselung, sowie des Hashings allgemeinverständlich erklären.			
Inhalt:			
- Entwicklung der Kryptographie, bekannte Fälle (Enigma), Motivation - Abgrenzung Steganographie - Mathematische Grundlagen			

- Symmetrische & asymmetrische Kryptographie
 - AES, DES, IDEA, PGP, RSA, Diffie-Hellmann, ElGamal, Elliptic Curve
 - Attacken, Brute Force, Rainbow Tables, Man-in-the-Middle
- Hashingverfahren
 - MD5, SHA-Familie, etc.
 - Secure Password Management
- Authentifizierungsverfahren, z.B. Challenge-Response, Zero-Knowledge-Verfahren
- Anwendung, z.B. in der Blockchain (Merkletree, Nonce)
- Praktikum/Übung: Angewandte Kryptographie
 - Einsatz und Übungen mit u.a. Cryptool (<https://www.cryptool.org/de/>), Hashgenerator (<https://hashgenerator.de/>)

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Bruce Schneier: Angewandte Kryptographie, 1. Auflage (1. Dezember 2005), Pearson Studium Verlag, ISBN: 978-3827372284
- Stephan Spitz et al.: Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen, 2. Auflage, überarb. Aufl. 2011 (24. Februar 2011), Vieweg+Teubner Verlag, ISBN: 978-3834814876
- Ronald Petrlic et al.: Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 1. Auflage (10. April 2017), Springer Vieweg Verlag, ISBN: 978-3658168384

Wirtschaftsenglisch			
Modulkürzel:	DIS-Wirtschaftsenglisch	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Lynne Gabbey		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Wirtschaftsenglisch		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Erwerb der Fähigkeit zur flüssigen sozialen Interaktion Handlungskompetenz: Fähigkeit die englische Sprache fach- und berufsbezogen im internationalen Kontext mündlich anzuwenden Sozialkompetenz: Verständnis von interkulturellen Faktoren			
Inhalt:			
• Ausbau von Grundfertigkeiten • Einführung in landeskundliche Aspekte des englischen Sprachraumes unter besonderer Berücksichtigung interkultureller Faktoren und Verhaltenskodizes • Fähigkeit flüssig und angemessen in Bezug auf geschäftliche Situationen zu kommunizieren (Face to Face) • Erwerb einer Sprechfertigkeit, die es erlaubt ohne Mühe die eigene Meinung klar und angemessen darzulegen (Meeting) • Fähigkeit schwierige und komplexere Themenstellungen nicht nur zu erfassen, sondern auch zusammenfassend wiederzugeben (Telephoning) • Übungen zu Textaufbau und Erstellen einer Präsentation • Graphs und Charts.			
Studien- / Prüfungsleistungen:			
Projektarbeit (außerhalb Prüfungszeitraum)			

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur

- Ergänzende Materialien werden über den Overhead-Projektor projiziert bzw. als Handouts verteilt.
- Im Sprachlabor werden Videos und Hörmaterialien eingesetzt.

Cyber Security			
Modulkürzel:	DIS-Cyber Security	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Cyber Security		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden vertiefen und verbreitern ihr Grundlagenwissen im Bereich der IT-Sicherheit und erhalten einen umfassenden Überblick über die wichtigsten Aspekte der IT-Sicherheit, was sie zur Teilnahme an weiterführenden, vertiefenden und praktischen Lehrveranstaltungen befähigt. Handlungskompetenz: Die Studierenden können fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit, sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von IT-Sicherheitswerkzeugen bzw. -Appliances, Methoden oder Konzepten aktiv mitwirken, um den operativen Betrieb einer Organisation möglichst sicher zu gestalten. Basierend auf der erworbenen Fachkompetenz können die Studierenden im 4. Fachsemester eine fundierte Wahl der Studienschwerpunkte treffen. Sozialkompetenz: Aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit, Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.			
Inhalt:			
• Sicherheit und Risikomanagement • Asset Security • Security Architecture and Engineering • Physische Sicherheit • Netzwerksicherheit			

- Firewalls und Intrusion Detection / Prevention
- Authentifizierung und Berechtigungsmanagement
- Betriebssystemsicherheit: Windows, Unix, Linux
- Sicherheit von mobilen Endgeräten
- Web Security und Anwendungssicherheit
- Datensicherung
- Incident Management
- Standards der Informationssicherheit

Studien- / Prüfungsleistungen:

Studienarbeit (außerhalb Prüfungszeitraum)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Secorvo (Herausgeber): Informationssicherheit und Datenschutz: Handbuch für Praktiker und Begleitbuch zum T.I.S.P., 3. Auflage 2019 (2. Oktober 2019), dpunkt Verlag, ISBN: 978-3864905964
- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren – Protokolle, 10th expanded and updated edition (21. August 2018), De Gruyter Verlag, ISBN: 978-3110551587
- Michael Bartsch et al.: Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, 1. Auflage 2018 (8. August 2018), Springer Vieweg Verlag, ISBN: 978-3658216542
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487

Compliance-Management			
Modulkürzel:	DIS-Compliance-Management	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Stefanie Fehr		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Compliance-Management		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die Auditprinzipien und sind in der Lage ein Audit mit den Schwerpunkten Datenschutz sowie Compliance zu konzipieren und zu managen. Ferner können sie zwischen internen, externen Audit sowie Zertifizierungen differenzieren. Den Studierenden sind die gängigen Formen eines Audits bekannt und sie können die üblichen Zertifizierungsverfahren benennen. Durch die praxisnahen Übungen festigen sich die konkreten Anwendungsfälle. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... den Begriff Audit zu definieren. • ... die Rolle des Auditors zu kennen. • ... zwischen (internen/externen) Audits und Zertifizierungen zu unterscheiden. • ... den Ablauf eines Audits zu konzipieren. • ... einen Fragenkatalog für ein Compliance- und Datenschutz-Audit zu entwickeln. Handlungskompetenz: Die Studierenden können ... • ... zwischen internen und externen Audits differenzieren. • ... die Schwierigkeiten bei der Durchführung von Audits erkennen und Handlungsoptionen ableiten. Sozialkompetenz: Die Studierenden können ... • ... einen Fragenkatalog für ein (Teil-) Audit entwickeln. • ... eigenständig ein (Teil-) Audit durchführen.			

Inhalt:
• Wesen, Arten und Planung von Audits • Vorbereitung, Durchführung und Nachbereitung eines Audits • Zertifizierungsverfahren • Qualifikationsanforderungen an Auditoren • Methodische Aspekte der Auditierung • Aktuelle Prüfungsstandards
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 60 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Brauweiler, J., Will, M. (2015): Auditierung und Zertifizierung von Managementsystemen. • Pachinger, M., Beham, G. (2020): Datenschutz-Audit: Recht - Organisation - Prozess - IT. • Roßnagel (1999): Datenschutzaudit: Konzeption, Durchführung, gesetzl. Grundlage. • Sowa, A., Duscha, P. et al. (2005): IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die ITPrüfung. • Graham, L. (2015): Internal Control Audit and Compliance: Documentation and Testing under the new COSO Framework.

Webentwicklung			
Modulkürzel:	DIS-Webentwicklung	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Michael Zilker		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Webentwicklung		
Lehrformen des Moduls:	DIS/WIF		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	Keine		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden erhalten die Kompetenz einfache Webanwendungen eigenständig zu entwerfen und umzusetzen. Sie sind in der Lage unterschiedlicher Web-Technologien zu verstehen, einzusetzen und in Kombination zu nutzen. Sie erhalten die Kompetenz Inhalte zu strukturieren und plausibel zu verlinken. Weiterhin sind die Studierenden befähigt Inhalte technisch aufzubereiten und in geeigneten Formaten abzuspeichern. Die Studierenden verfügen über die Fähigkeit einfache 2D-Animationen zu gestalten. Sie verfügen über die Kompetenz komplexere Anwendungssysteme, die auf Content Managementsystemen basieren, individuell hinsichtlich Layouts und Funktionalitäten auszurichten und zu gestalten. Handlungskompetenz Die Studierenden erhalten die Kompetenz zielgerichtet Entwicklungswerkzeuge auszuwählen und diese professionell zu nutzen. Sie sind in der Lage statische Web-Anwendungen komplett umzusetzen. Die Studierenden erwerben die Kompetenz komplexe Web-Anwendungen technisch einzuordnen und hinsichtlich einer technischen und gestalterischen Modifikation zu beurteilen.			
Inhalt:			
Begriffsdefinition und generelle Einsatzmöglichkeiten von Multimedia- und Internetanwendungen. Beschreibungssprachen zur Darstellung von Inhalten im Internet (HTML) und Arbeiten mit einschlägigen Entwicklungstools. Darstellung einer Sprache zur Text-, Webseiten- und Bildformatierung, hier Cascading Stylesheets (CSS). Bildbearbeitungssoftware zur Aufbereitung von Bildern für das Web. Grundlegende Techniken zur Bildbearbeitung. Programmiersprachen zur Umsetzung von Funktionalitäten und interaktiven Abfragen auf dem Client, hier JavaScript. Einsatz von Programmierframeworks. Grundlegende Programmierkonzepte dieser Sprache sowie spezifische Eigenschaften und Methoden innerhalb des zugrunde gelegten			

Objektmodells.

Anlegen von bewegten interaktiven Web-Elementen unter Verwendung von einschlägigen Werkzeugen. Aufbau einer, auf einem Content Management System basierenden, Web-Anwendung. Modifikation der bereitgestellten Basisfunktionen durch Programmierung.

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Münz, Gull: HTML Handbuch Franzis Verlag, jeweils neueste Auflage
- Ackermann: JavaScript, Rheinwerk Computing
- Wenz: JavaScript, Galileo Computing, jeweils neueste Auflage
- Laborenz: CSS-Praxis, Galileo Verlag, jeweils neueste Auflage
- Videotutorials laut aktueller Empfehlung
- Webseiten laut aktueller Empfehlung, z.B.: www.selfhtml.org

Privacy Engineering			
Modulkürzel:	DIS-Privacy Engineering	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Privacy Engineering		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	Keine		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden haben einen umfassenden Überblick über die wichtigsten technische und Design-Werkzeuge für den Schutz der Privatsphäre. Sie kennen die wichtigsten Grundprinzipien des Datenschutzes, und sie sind in der Lage geeignete Privacy Policies für eine Organisation zu definieren und Datenschutz-Anforderungen für neue Anwendungen zu sammeln. Die Studierenden können danach eine Lösung entwickeln, die die Privatsphäre des Nutzers während des gesamten Lebenszyklus schützt. Handlungskompetenz Die Studierenden können im Rahmen der Entwicklung von Privacy Policies und neue Lösungen in einer Organisation Empfehlungen für die Auswahl geeigneter Anforderungen und technischen Werkzeugen aussprechen. Aufgrund des erworbenen Grundwissens sind sie in der Lage, auch zukünftige technische und gesetzliche Entwicklungen in diesen Bereichen einzuordnen und zu bewerten. Sozialkompetenz Die Studierenden vertiefen die Kompetenz sich in Projektteams zu integrieren. Die Studierenden können mit Rechtsexperten in einem Team zusammenarbeiten und in einer einfachen Sprache kommunizieren, um eine effiziente Lösung zur Wahrung der Privatsphäre zu entwickeln.			
Inhalt:			
• Herkunft: Privacy-by-Design, Privacy Engineer's Manifesto, Privacy Engineering • Herausforderungen: Ingenieure und Rechtsexperten, rechtliche Unterschiede in der Rechtsprechung, kulturelle Sicht der Privatsphäre • Grundprinzipien des Datenschutzes: GAPP, OECD Guidelines, FIPPs, ISO 2700x Series			

- Privacy Policies Entwicklung
- Datenschutz Anforderungen Sammlung
- Einwilligung bei der Aufnahme personenbezogener Daten
- Datenschutz während des gesamten Lebenszyklus: die Lebenszyklus-Methodik, Use Cases, Unified Modelling Language (UML)
- Privacy Engineering und Qualität
- Technische Werkzeuge und Design für den Schutz der Privatsphäre: Sicherheit, Anonymität, Autonomie und Transparenz

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Michelle Dennedy, et al.: The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value, Apress Verlag, 1. Auflage (27. Januar 2014), ISBN: 978-1430263555
- Kranig T., Sachs, A., Gierschmann, M.: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2017, ISBN: 978-3846207604
- Ian Oliver: Privacy Engineering: A Dataflow and Ontological Approach, CreateSpace Independent Publishing Platform; 1. Auflage (18. Juli 2014), ISBN: 978-1497569713
- Aurelia Tamò-Larrieux: Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things, Springer Verlag, 1. Auflage 2018 (13. November 2018), ISBN: 978-3319986234
- <https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/about>

Cloud-Computing			
Modulkürzel:	DIS-Cloud-Computing	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Cloud-Computing		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die Grundlagen zum Erstellen von IT-Infrastrukturen in Public Clouds (am Beispiel von Amazon AWS, Google GCP und Microsoft Azure). Sie sind in der Lage, Dienste von Public Clouds zu bedienen und über programmatische Techniken zu kombinieren und zu automatisieren. Durch die praxisnahen Übungen und Fallstudien sind die Studierenden mit der Anwendung vertraut. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... die Anwendungsparadigmen und Dienste der Public Cloud zu benennen und diese im Kontext einzuordnen. • ... eigenständig geeignete Cloud-Dienste auszuwählen und diese zu konfigurieren und zu verwalten. • ... moderne Anwendungsarchitekturen auf Basis von Cloud Native Techniken zu beschreiben und einzusetzen. • ... Cloud-Dienste zu automatisieren und abzusichern. Handlungskompetenz: Die Studierenden können ... • ... Public und Private Cloud Dienste umfassend bedienen. • ... IT-Architekturen für die Bereitstellung von Anwendungen in der Public Cloud umsetzen. Sozialkompetenz: Die Studierenden können ... • ... komplexe Problemstellungen aus dem Bereich der IT-Infrastruktur und des Applikationsdesigns im Team erörtern. • ... die Fähigkeit zum Zeitmanagement verbessern.			

Inhalt:
Noch zu bestimmen
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 60 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.
Literatur: Wird zu Beginn bekannt gegeben

IT-Sicherheitsmanagement			
Modulkürzel:	DIS-IT-Sicherheitsmanagement	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	IT-Sicherheitsmanagement		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die gängigen Standards im Bereich des IT Sicherheitsmanagements. Sie können Risikoanalysen durchführen und ein Notfallmanagement konzipieren und etablieren. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... die Aufgaben des IT Sicherheitsmanagements zu benennen. • ... Risikoanalysen durchzuführen. • ... ein Notfallmanagement zu konzipieren und zu etablieren. Handlungskompetenz: Die Studierenden können ... • ... die BSI Grundschutz-Methode anwenden. • ... die Eigenschaften sicherer Netzwerkarchitekturen benennen. • ... Audits planen. • ... Notfallmanagement konzipieren. Sozialkompetenz: Die Studierenden können ... • ... komplexe Problemstellungen aus dem Bereich des IT-Sicherheitsmanagements im Team erörtern. • ... ihre Präsentationsfähigkeiten verbessern. • ... die Fähigkeit zum Zeitmanagement verbessern.			
Inhalt:			
• Einführung in die ISO/IEC 27001-Familie • Weitere IT-Sicherheitsmanagementsysteme (ISMS), z.B. BSI Grundschutz, ISIS12			

- Einführung, Planung, Betrieb, Verbesserung, PDCA-Zyklus
- Zertifizierung von Personen und Organisationen
- Einbindung in das IT-Servicemanagement & Datenschutzmanagement

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 60 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Michael Brenner, et al.: Praxisbuch ISO/IEC 27001 – Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, 2. Auflage, neu bearbeitet und erweitert, Hanser Verlag, 2017, ISBN: 978-3446451391
- Thomas W. Harich: IT-Sicherheitsmanagement: Praxiswissen für IT Security Manager, mitp Verlag, 2. Auflage 2018 (30. Juni 2018), 978-3958452732
- Jaqueline Naumann; Ihr Kampf als Informationssicherheitsbeauftragter (ISB) (Die ganze Härte der ISO 27001), Books on Demand Verlag; 2. Auflage (18. September 2018), ISBN: 978-3746091303

Projektmanagement			
Modulkürzel:	DIS-Projektmanagement	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Jonas Härtfelder		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Projektmanagement		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS * WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden erlernen die wesentlichen Methoden des Projektmanagements, das für die Leitung von Projekten erforderlich ist. Handlungskompetenz Die Studierenden können mit gängigen Projektmanagementmethoden und -Werkzeugen umgehen.			
Inhalt:			
Project Management: • Core functions: Scope Mgmt, Time Mgmt, Cost Mgmt, Quality Mgmt • Facilitating functions: Human Resources Mgmt, Communication Mgmt, Risk Mgmt, Procurement Mgmt • Project Integration Management • Microsoft Project (Anwendung)			
Studien- / Prüfungsleistungen:			
schriftliche Prüfung, 90 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Brewer, J. & Dittman, K. (2009). Methods of IT Project Management. Prentice Hall. ISBN: 0132367254. • Schwalbe, K. (2009). Information Technology Project Management. Cengage Learning Services. ISBN:			

032478855X.

- Marchewka, J. T. (2009). Information Technology Project Management. Wiley. ISBN: 0470409487.

Datenschutzfolgenabschätzung mit Risikomanagement			
Modulkürzel:	DIS-Datenschutzfolgenabschätzung m.RM	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Stefanie Fehr		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Datenschutzfolgenabschätzung mit Risikomanagement		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden haben ein Verständnis vom Risikomanagement und können dies im Kontext des Datenschutzes anwenden. Sie sind in der Lage, methodisch sicher eine Datenschutzfolgeabschätzung durchzuführen. Ferner sind sie mit den datenschutzrechtlichen Grundlagen und Standards im Kontext der Datenschutzfolgeabschätzung vertraut. Durch die praxisnahen Übungen in Form eines Planspiels sind die Studierenden mit der Anwendung auf konkrete Sachverhalte vertraut. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... eigenständig Risiken zu identifizieren. • ... eigenständig eine Risikoanalyse durchzuführen. • ... Schritte zur Vorbereitung auf die Datenschutzfolgeabschätzung zu benennen und diese im Kontext einzuordnen. • ... die Phasen der Datenschutzfolgeabschätzung zu durchlaufen und diese eigenständig durchzuführen. Handlungskompetenz: Die Studierenden können ... • ... im Anwendungsfall die Risiken erkennen und hieraus Folgemaßnahmen ableiten. • ... im Anwendungsfall die Notwendigkeit einer Datenschutzfolgeabschätzung benennen sowie die Folgeschritte einleiten. Sozialkompetenz: Die Studierenden können ...			

• ... die Risiken definieren und hieraus Handlungsschritte ableiten. • ... eigenständig eine Datenschutzfolgeabschätzung durchführen.
Inhalt:
• Definition Strategisches Risikomanagement • Risiken im Sinne der DSGVO • Durchführung von Risikoidentifikation und -analysen • Begriffsbestimmung Datenschutzfolgeabschätzung • Verantwortlichkeit für die Datenschutzfolgeabschätzung • Notwendige Vorarbeiten (Tätigkeiten, Beteiligte, etc.) • Phasen einer Datenschutzfolgeabschätzung • Zusatz: Planspiel Datenschutzfolgeabschätzung
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Martin, N., Friedewald, M. et al. (2020): Die Datenschutz-Folgeabschätzung nach Art. 35 DSGVO • Romeike, F. (2018): Risikomanagement. • Vanini, U. (2021): Risikomanagement: Grundlagen Instrumente Unternehmenspraxis. • Kühling, J., Klar, M., Sachmann, F. (2018): Datenschutzrecht. • Eßner, M., Franck, L. (2021): Datenschutzrecht: Fälle und Lösungen.

Gesetze, Institutionen und Aufgaben			
Modulkürzel:	DIS-Gesetze, Institutionen und Aufgaben	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Stefanie Fehr		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Gesetze, Institutionen und Aufgaben		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden verfügen über Kenntnisse des deutschen Verfassungsrechts und seinen Bezügen zum Europarecht. Sie kennen die verfassungsrechtlich geschützten wirtschaftsrelevanten Grundrechte und sind in der Lage, Eingriffe in diese Grundrechte methodisch korrekt zu beurteilen. Sie erkennen die stetig wachsende Bedeutung des europäischen Primär- und Sekundärrechts im Datenschutz und sind in der Lage, Verstöße gegen europäisches Sekundärrecht zu erkennen methodisch korrekt zu prüfen. Die Übung unterstützt die methodische Anwendung der gelernten Inhalte auf konkrete Sachverhalte. Fach- und Methodenkompetenz: Die Studierenden werden befähigt • ... die Begriffe und Funktionen des Rechts zu definieren. • ... die Grundrechte im Kontext des Datenschutzes zu erläutern und daraus Grundrechtseingriffe abzuleiten, z. B. informationelle Selbstbestimmung. • ... die Gesetzgebungsverfahren auf nationaler und europäischer Ebene zu benennen. • ... die Zuständigkeit von Institutionen in Bezug auf Datenschutz zu bestimmen. Handlungskompetenz: Die Studierenden können ... • ... im Anwendungsfall Grundrechtseingriffe definieren und die Folgen ableiten. • ... im Anwendungsfall die Zuständigkeit der jeweiligen Institution benennen und ihre Eingriffsbefugnis definieren. • ... aktuelle Gesetzgebungsverfahren den jeweiligen Ebenen zu ordnen (National oder Europa). Sozialkompetenz: Die Studierenden können ...			

- ... methodisch Sachverhalte im Kontext des Moduls prüfen und anwenden.
- ... den aktuellen Diskussionen um Gesetzgebungsverfahren folgen.

Inhalt:

- Grundzüge des Staatsorganisationsrechts (z.B. Gesetzgebungs- und Verwaltungskompetenzen)
- Wirtschaftsordnung und Grundgesetz (allgemein)
- wirtschaftsrelevante Grundrechte (Eigentumsschutz, Berufsfreiheit, Koalitionsfreiheit, Gleichheitssatz) und sonstige wirtschaftlich relevante Grundrechte und Verfassungsprinzipien
- Grundzüge des Europarechts; europäische Grundfreiheiten und europäisches Sekundärrecht am Beispiel der DSGVO
- Mit dem Datenschutz & IT-Sicherheit befassten Institutionen und ihrer Aufgaben sowie Zuständigkeiten
- Zusammenwirken der Institutionen, insb. auch bei grenzübergreifenden Organisationen

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 60 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Schliesky, U. (2014): Öffentliches Wirtschaftsrecht.
- Piero, B., Schlink, B. (2005): Staatsrecht II – Grundrechte.
- Gleixner, A. (2018): Staatliche Durchsetzung von Datenschutz: Die Institution des Landes- (und Bundes-) Datenschutz.
- Hauser, W., Unger, K. (2015): Grundzüge des Datenschutzrechts.
- Rosenmayr-Klemenz, C., Bogendorfer, R. (2018): EU-Datenschutzgrundverordnung und Datenschutz-Anpassungsgesetz

Unternehmensauditierung			
Modulkürzel:	DIS-Unternehmensauditierung	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	7	
Modulverantwortliche(r):	Prof. Dr. Stefanie Fehr		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Unternehmensauditierung		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	Keine		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die Auditprinzipien und sind in der Lage ein Audit mit den Schwerpunkten Datenschutz sowie Compliance zu konzipieren und zu managen. Ferner können sie zwischen internen, externen Audit sowie Zertifizierungen differenzieren. Den Studierenden sind die gängigen Formen eines Audits bekannt und sie können die üblichen Zertifizierungsverfahren benennen. Durch die praxisnahen Übungen festigen sich die konkreten Anwendungsfälle. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... den Begriff Audit zu definieren. • ... die Rolle des Auditors zu kennen. • ... zwischen (internen/externen) Audits und Zertifizierungen zu unterscheiden. • ... den Ablauf eines Audits zu konzipieren. • ... einen Fragenkatalog für ein Compliance- und Datenschutz-Audit zu entwickeln. Handlungskompetenz: Die Studierenden können ... • ... zwischen internen und externen Audits differenzieren. • ... die Schwierigkeiten bei der Durchführung von Audits erkennen und Handlungsoptionen ableiten. Sozialkompetenz: Die Studierenden können ... • ... einen Fragenkatalog für ein (Teil-) Audit entwickeln. • ... eigenständig ein (Teil-) Audit durchführen.			

Inhalt:
• Wesen, Arten und Planung von Audits • Vorbereitung, Durchführung und Nachbereitung eines Audits • Zertifizierungsverfahren • Qualifikationsanforderungen an Auditoren • Methodische Aspekte der Auditierung • Aktuelle Prüfungsstandards
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten (im Antwort-Wahl-Verfahren gem. § 8 c APO) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Brauweiler, J., Will, M. (2015): Auditierung und Zertifizierung von Managementsystemen. • Pachinger, M., Beham, G. (2020): Datenschutz-Audit: Recht - Organisation - Prozess - IT. • Roßnagel (1999): Datenschutzaudit: Konzeption, Durchführung, gesetzl. Grundlage. • Sowa, A., Duscha, P. et al. (2005): IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die ITPrüfung. • Graham, L. (2015): Internal Control Audit and Compliance: Documentation and Testing under the new COSO Framework.

Professionelle Kommunikation			
Modulkürzel:	DIS-Professionelle Kommunikation	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	7	
Modulverantwortliche(r):	N.N.		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Professionelle Kommunikation		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	Keine		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden beherrschen Kenntnisse in der Problemanalyse und Entwicklung von Vorgehensweisen im kommunikativen Umgang mit Projektpartnern und Teilöffentlichkeiten. Handlungskompetenz • Konzeptentwicklung allgemein Kampagnen einordnen und entwickeln • Modelle zur Einordnung von Konfliktsituationen • Interventions- und Konfliktmanagementmethoden • Konfliktverhalten • Mitarbeiter-, Führungskräfte- und Change-Kommunikation Sozialkompetenz Medienkompetenz / Kommunikationsfähigkeit / Empathie / Emotionale Kompetenz / Konfliktfähigkeit / Problemlösungskompetenz			
Inhalt:			
• Was bedeutet professionelle Kommunikation? • Vorbereitung auf den Krisenfall • Grundzüge der medialen Logik bei Risiken und Krisen, erwartete und unerwartete Auswirkungen • Wie verhalte ich mich richtig vor der Kamera? • Souveräne Reaktion auf journalistische Fragestellungen. • Praktische Übungen vor der Kamera mit Aufnahme und Analyse			

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

Wird zu Beginn bekannt gegeben

2.2 Praktisches Studiensemester

Betriebliche Praxis			
Modulkürzel:	Betriebliche Praxis	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	6	
Modulverantwortliche(r):	Prof. Dr. Wolf Knüpffer		
Sprache:	Deutsch		
Leistungspunkte / SWS:	18 ECTS / 0 SWS		
Arbeitsaufwand:	Kontaktstunden:	0 h	
	Selbststudium:	540 h	
	Gesamtaufwand:	540 h	
Moduldauer:	1 Semester		
Häufigkeit:	Winter- und Sommersemester		
Lehrveranstaltungen des Moduls:	Betriebliche Praxis		
Lehrformen des Moduls:	Praktikum		
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.		
Empfohlene Voraussetzungen:	Teil I und Teil II des Bachelorstudiums		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden erwerben im Praktikum individuelle Fachkenntnisse aus dem jeweils anstehenden Aufgabenfeld. Thematisch sollte die, im Studium erworbene Fachkompetenz, durch konkrete betriebliche Tätigkeiten gefestigt und erweitert werden. Handlungskompetenz Die Studierenden erwerben die Kompetenz Aufgaben aus der betrieblichen Praxis des Datenschutzes und der IT-Sicherheit zu übernehmen und zu bearbeiten. Dabei erwerben sie die Fähigkeit Entscheidung im gesetzten Rahmen zu treffen und zu verantworten Sozialkompetenz Die Studierenden erwerben die Kompetenz im betrieblichen Team zu arbeiten. Dabei erlangen sie die Fähigkeit eigene Ideen in Gruppen zu kommunizieren und nach Möglichkeit durchzusetzen. Die Studierenden erlangen die Kompetenz sich mit anderen Personen abzustimmen und durch die Kommunikation Synergieeffekte zu generieren.			
Inhalt:			
Die Studierenden sollen entsprechend ihrer zukünftigen Ausrichtung an Aufgaben mitarbeiten und Teilaufgaben selbstverantwortlich ausführen, deren Schwierigkeitsgrad dem Ausbildungsstand und den späteren Anforderungen in der betrieblichen Praxis angemessen ist.			

Studien- / Prüfungsleistungen:
TN Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Keine Anmerkungen

Praxisseminar			
Modulkürzel:	Praxisseminar	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	6	
Modulverantwortliche(r):	Prof. Dr. Michael Schugk		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Praxisseminar		
Lehrformen des Moduls:	S - Seminar		
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.		
Empfohlene Voraussetzungen:	Teil I und Teil II des Bachelorstudiums		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fachkompetenz			
• Kenntnis und Verstehen wichtiger Ansätze / Methoden / Modelle zur Verbesserung der interpersonalen Kommunikation			
Methodenkompetenz			
• Erkennen der Bedeutung der dargelegten Ansätze und Modelle für die berufliche Kommunikation			
• Befähigung zur Einbringung des erlangten Wissens in das eigene Kommunikationsverhalten			
Sozialkompetenz			
• Verbesserung der eigenen Kommunikation und Metakommunikation			
• Erlangung von Effektivität, Effizienz und Humanität im eigenen Kommunikationsverhalten			
• Verbessertes Erkennen des eigenen / fremden Kommunikationsverhaltens			
• Erlangung höheren Bewusstseins über das eigene / fremdes Kommunikationsverhalten			
Inhalt:			
• Hamburger Verständlichkeitskonzept			

- Verhandlungsführung nach dem Harvard-Konzept
- Transaktionsanalyse nach Eric Berne
- Menschliche Verhaltenssteuerung
- Kommunikationspsychologie nach Friedmann Schulz von Thun

Studien- / Prüfungsleistungen:

Teilnahme und Referat (außerhalb Prüfungszeitraum)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Langer, Inghard; Schulz von Thun, Friedemann; Tausch, Reinhard: Sich verständlich ausdrücken. 10. völlig neubearbeitete Auflage. München: Ernst Reinhardt Verlag, 2015.
- Fisher, Roger; Ury, William; Patton, Bruce: Das Harvard-Konzept. Sachgerecht verhandeln – erfolgreich verhandeln. 20. Auflage. Frankfurt; New York: Campus Verlag GmbH, 2001
- Berne, Eric: Spiele der Erwachsenen. Psychologie der menschlichen Beziehungen. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag GmbH, 1991.
- Stewart, Ian; Joines, Vann: Die Transaktionsanalyse. Eine Einführung. 12. Auflage. Freiburg: Verlag Herder Freiburg im Breisgau, 2000.
- Häusel, Hans-Georg: Think Limbic! Die Macht des Unbewussten für Management und Verkauf. Freiburg: Haufe-Lexware GmbH & Co. KG, 2014.
- Schulz von Thun, Friedemann: Miteinander reden 1. Störungen und Klärungen. Allgemeine Psychologie der Kommunikation. Hamburg: Rowohlt Taschenbuch Verlag GmbH, Sonderausgabe April 2011.
- Schulz von Thun, Friedemann: Miteinander reden 3. Das "Innere Team" und situationsgerechte Kommunikation. Hamburg: Rowohlt Taschenbuch Verlag GmbH, Sonderausgabe April 2011.

Praxisbegleitende Lehrveranstaltung (wissenschaftliches Arbeiten)			
Modulkürzel:	praxisbegl. Lehrveranstaltung	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	6	
Modulverantwortliche(r):	Prof. Dr. Michael Zilker		
Sprache:	Deutsch		
Leistungspunkte / SWS:	3 ECTS / 2 SWS		
Arbeitsaufwand:	Kontaktstunden:	23 h	
	Selbststudium:	68 h	
	Gesamtaufwand:	91 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Praxisbegleitende Lehrveranstaltung (wissenschaftliches Arbeiten)		
Lehrformen des Moduls:	SU - seminaristischer Unterricht		
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.		
Empfohlene Voraussetzungen:	Teil I und Teil II des Bachelorstudiums		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden kennen die fachlichen Anforderungen an wissenschaftliche Abschlussarbeiten und mögliche Strategien, um diese zu erfüllen. Die Studierenden haben im Rahmen eines Arbeitsmusters bereits erste Erfahrungen mit wissenschaftlichem Arbeiten gemacht und kennen die typische Struktur einer wissenschaftlichen Abschlussarbeit. Handlungskompetenz Die Studierenden sind in der Lage eine erste wissenschaftliche Arbeit erfolgreich zu erstellen. Die Studierenden können selbständig korrekt zitieren und zielorientiert recherchieren. Sozialkompetenz Die Studierenden können ihren KommilitonInnen ihre wissenschaftliche Fragestellung schildern und im Team Lösungsstrategien entwickeln.			
Inhalt:			
Die Lehrveranstaltung dient zur Vorbereitung auf die Bearbeitung des Bachelor-Projekts und der Bachelorarbeit. Grundlegende Methoden und Verfahren des wissenschaftlichen Arbeitens werden erläutert und anhand eines Arbeitsmusters eingeübt.			

Studien- / Prüfungsleistungen:

Teilnahme und Referat/StA

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient, 2016

Bachelor-Projekt			
Modulkürzel:	Bachelorpr Projekt	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	6	
Modulverantwortliche(r):	ProfessorInnen DIS		
Sprache:	Deutsch		
Leistungspunkte / SWS:	4 ECTS / 2 SWS		
Arbeitsaufwand:	Kontaktstunden:	23 h	
	Selbststudium:	98 h	
	Gesamtaufwand:	121 h	
Moduldauer:	1 Semester		
Häufigkeit:	Winter- und Sommersemester		
Lehrveranstaltungen des Moduls:	Bachelor-Projekt		
Lehrformen des Moduls:	PA - Projektarbeit		
Teilnahmevoraussetzung:	Als Zulassungsvoraussetzung für Module aus der Modulgruppe „Praktisches Studiensemester“ müssen mindestens 120 ECTS-Punkte erzielt worden sein.		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Handlungskompetenz Die Studierenden erwerben die Kompetenz ein Projekt zur Vorbereitung ihrer Bachelorarbeit eigenständig und zielgerichtet zu definieren und ganz oder teilweise umzusetzen. Dabei erwerben sie die Fähigkeit Projekte zu dokumentieren und zu präsentieren. Sozialkompetenz Die Teilnehmer erwerben die Kompetenz vor einem kleineren Auditorium ein Projekt zu präsentieren und zu verteidigen. Dabei erlangen sie die Fähigkeit der Gruppe zu kommunizieren und zu diskutieren.			
Inhalt:			
- Planung und Umsetzung von individuellen Projekten aus dem Bereich des Datenschutzes und der IT-Sicherheit. - Gestaltung von Präsentationen mit entsprechenden Visualisierungsprogrammen. - Präsentationstechniken und Gestaltung von Vorträgen. - Präsentation von Ergebnissen und oder Teilergebnissen auslaufenden Praxisprojekten. Darstellung aktueller Themen aus Projekten.			

Studien- / Prüfungsleistungen:
Projektarbeit (außerhalb Prüfungszeitraum) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Keine Anmerkungen

2.3 Bachelorarbeit

Bachelorarbeit			
Modulkürzel:	Bachelorarbeit	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	7	
Modulverantwortliche(r):	ProfessorInnen DIS		
Sprache:	Deutsch/Englisch		
Leistungspunkte / SWS:	12 ECTS / 0 SWS		
Arbeitsaufwand:	Kontaktstunden:	0 h	
	Selbststudium:	360 h	
	Gesamtaufwand:	360 h	
Moduldauer:	1 Semester		
Häufigkeit:	Winter- und Sommersemester		
Lehrveranstaltungen des Moduls:	Bachelorarbeit		
Lehrformen des Moduls:	BAr - Bachelorarbeit		
Teilnahmevoraussetzung:	Die Ausgabe des Themas der Bachelorarbeit setzt die erfolgreiche Ableistung von Modulen im Gesamtumfang von 160 ECTS-Punkten voraus.		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Handlungskompetenz Befähigung zur Anfertigung einer wissenschaftlichen Arbeit basierend auf einem praktischen Projekt. Hinführen zum selbstständigen wissenschaftlichen Arbeiten.			
Inhalt:			
Das Thema der Bachelorarbeit wird individuell aus dem Bereich des Themengebietes des Datenschutzes und der IT-Sicherheit gewählt. Die theoretische Arbeit wird auf der Grundlage eines praktischen Projektes formuliert und zeigt die aktuellen Fragestellungen des gewählten Themas sowie deren Lösungsansätze und -wege im Kontext des Projektes auf.			
Studien- / Prüfungsleistungen:			
Bachelorarbeit (außerhalb Prüfungszeitraum) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Heesen, Wissenschaftliche Arbeiten schreiben mit Word 2016, Prescient Verlag, 2016			

Bachelorseminar			
Modulkürzel:	Bachelorseminar	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	7	
Modulverantwortliche(r):	ProfessorInnen DIS		
Sprache:	Deutsch		
Leistungspunkte / SWS:	3 ECTS / 2 SWS		
Arbeitsaufwand:	Kontaktstunden:	23 h	
	Selbststudium:	68 h	
	Gesamtaufwand:	91 h	
Moduldauer:	1 Semester		
Häufigkeit:	Winter- und Sommersemester		
Lehrveranstaltungen des Moduls:	Bachelorseminar		
Lehrformen des Moduls:	Teilnahme und Referat		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Grundkenntnisse des wissenschaftlichen Arbeitens		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Handlungskompetenz Die Studierenden erhalten die Kompetenz den Hergang ihre Bachelorarbeit in unterschiedliche Entwicklungsstufen zu beleuchten und wissenschaftlich darzustellen. Sozialkompetenz Die Teilnehmer erlangen weiterhin die Kompetenz ihre Arbeit fachlich fundiert in einem studentischen Plenum zu präsentieren und zu verteidigen.			
Inhalt:			
• Präsentation von Zwischen- und Endergebnissen • Diskussion von Thesen • Diskussion von Ergebnissen • Fortentwicklung von wissenschaftlichen Arbeiten • Wissenschaftliches Arbeiten			
Studien- / Prüfungsleistungen:			
Teilnahme und Referat (außerhalb Prüfungszeitraum) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.			

Keine Anmerkungen

2.4 Spezialisierungen

Biometrie

Biometrie: Praktikum			
Modulkürzel:	SPM-Biometrie: Praktikum	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Biometrie: Praktikum		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Modul: Einführung in die IT-Sicherheit, grundlegende Programmierkenntnisse		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden können aktuelle Einsatz-Szenarien von biometrischen Systemen implementieren und evaluieren. Handlungskompetenz Die Studierenden sind in der Lage, aktuelle Herausforderungen biometrischen Systemen zu verstehen, analysieren, evaluieren und diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Sozialkompetenz Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen diskutieren. Darüber hinaus können die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.			
Inhalt:			
• Durchführung praktischer Übungen der Biometrie • Aktuelle Einsatz-Szenarien von biometrischen Systemen werden analysiert			

- Fragen der Interoperabilität und Standardisierung untersucht.
- Andere aktuelle Forschungsthemen auf dem Gebiet der Biometrie werden ferner behandeln

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- S. Li, A.K. Jain, Handbook of Face Recognition, Springer, (2011)
- D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, (2009)
- J. Wayman, A. Jain, D. Maltoni, D. Maio, Biometric Systems, Springer, (2005)
- Forschungsartikel in peer-reviewed Konferenzen oder Journalen

Biometrische Erkennung			
Modulkürzel:	SPM-Biometrische Erkennung	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Biometrische Erkennung		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden sollen das Verständnis für die Prinzipien und Verfahren in der Biometrie entwickeln und die wichtigsten biometrischen Verfahren kennenlernen. Darüber hinaus sollen sie die Sicherheitseigenschaften eines biometrischen Systems und komplexe Beziehungen zwischen Verfahren und Umgebungseinflüssen (z.B. Beleuchtungssituationen, Posenvariation etc.) herstellen und deren Auswirkung auf die Erkennungsleistung von Systemen bewerten können. Handlungskompetenz Die Studierenden sollen für einen vorgegeben Anwendungsbereich geeignete Verfahren auswählen können und eine ausgewogene Balance zwischen Technologie und Grundprinzipien des Datenschutzes entwickeln.			
Inhalt:			
• Mechanismen der wichtigsten biometrischen Verfahren, die heute in kommerziellen Systemen zum Einsatz kommen (Fingerbilderkennung, Gesichtserkennung, Iriserkennung) • die Methoden der Sensorik, Signalverarbeitung, Merkmalsextraktion und Klassifikation			

- Bewertungskriterien zur Auswahl von biometrischen Systemen: Erkennungsleistung vs. Sicherheitseigenschaften
- Grundzüge der im Kontext von biometrischen Systemen relevanten Datenschutzprinzipien

Studien- / Prüfungsleistungen:

Schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- S. Li, A.K. Jain, Handbook of Face Recognition, Springer, (2011)
- D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, (2009)
- J. Wayman, A. Jain, D. Maltoni, D. Maio, Biometric Systems, Springer, (2005)

Forschungsartikel in peer-reviewed Konferenzen oder Journalen

IT- Infrastruktur

IT-Planung und Administration			
Modulkürzel:	SPM-IT-Planung und Administra- tion	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	IT-Planung und Administration		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS/WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden verfügen über detaillierte Kenntnisse der typischen administrativen Aufgaben und Abläufe, die im Kontext des Betriebs eines modernen Betriebssystems anfallen. Weiterhin verfügen die Studierenden über ein Grundverständnis bzgl. der Zusammenhänge und Abläufe innerhalb eines modernen Betriebssystems. Die Studierenden können grundlegende Zusammenhänge zwischen administrativen Tätigkeiten und dem Management des IT-Betriebs erkennen. Handlungskompetenz: Die Studierenden können die administrativen Kernaufgaben der Einrichtung und Administration eines modernen Betriebssystems in typischen Einsatzszenarien selbstständig durchführen. Weiterhin können die Studierenden aktiv an der Planung, Realisierung und Leitung eines IT-Betriebs teilnehmen. Sozialkompetenz: Die Studierenden können sowohl mit IT-Fachleuten, als auch mit Fachanwendern effektiv und situationsgerecht kommunizieren. Sie sind geübt in der Zusammenarbeit in kleinen bis mittleren Teams und kennen grundlegende Strategien der Arbeitsteilung.			

Inhalt:
Vermittlung der typischen Administrations- und Planungsaufgaben für den Betrieb eines modernen Betriebssystems und Vertiefung der Lehrinhalte durch praktische Übungen am Rechner. Behandlung von grundlegenden Planungsstrategien für mittlere bis große Netzwerkinstallationen und Vertiefung der Lehrinhalte durch Fachdiskussionen auf Basis von typischen Beispielszenarien.
Studien- / Prüfungsleistungen:
mündliche Prüfung, 20 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.
Literatur: • Unterlagen der Red Hat IT Academy • Microsoft Corp.: 21410B: Installieren und Konfigurieren von Windows Server 2012 (Kursunterlagen, MS ITAcademy) • Joos, Thomas: Microsoft Windows Server 2016 - Das Handbuch: Von der Planung und Migration bis zur Konfiguration und Verwaltung. O'Reilly Verlag, 1. Auflage 2017, ISBN: 978-3960090182

IT-Service-Management			
Modulkürzel:	SPM-IT-Service-Management	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Sascha Müller-Feuerstein		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	IT-Service-Management		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS/WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden verfügen über ein umfassendes Basiswissen im Bereich IT-Service-Management (ITSM). Neben den Grundkonzepten des ITSM kennen Sie die wichtigsten Prozesse, Rollen und Problembereiche des Betriebs mittlerer bis großer IT-Infrastrukturen. Handlungskompetenz: Die Studierenden verfügen über die Fähigkeit typische Problem mittlerer und großer IT-Betriebe zu erkennen und durch den Einsatz von Best-Practice-Methoden im Bereich ITSM gezielt auf deren Lösung hinzuwirken. Sozialkompetenz: Die Studierenden können sowohl mit IT-Fachleuten, als auch mit Fachanwendern effektiv und situationsgerecht kommunizieren. Sie sind geübt in der Zusammenarbeit in kleinen bis mittleren Teams und kennen grundlegende Strategien der Arbeitsteilung.			
Inhalt:			
Umfassender Einblick in die wichtigsten IT-Service-Managementprozesse eines IT-Betriebs, basierend auf dem ITBest-Practice-Rahmenwerk IT Infrastructure Library (ITIL). Am Rande werden zudem ISO 20k, CoBIT und ISO 27001 behandelt. Neben den Prozessdefinitionen werden u.a. die kritischen Erfolgsfaktoren, Rollen,			

Kennzahlen und Schnittstellen der ITIL-Kernprozesse im Detail behandelt und durch Fallstudien weiter vertieft. Optional ist die Teilnahme an einer zusätzlichen und kostenpflichtigen ITIL-Foundation-Zertifizierungsprüfung möglich.

Studien- / Prüfungsleistungen:

Studienarbeit (außerhalb Prüfungszeitraum)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Böttcher, Roland: IT-Service-Management mit ITIL® - 2011 Edition: Einführung, Zusammenfassung und Übersicht der elementaren Empfehlungen. Heise Verlag, 3. Auflage, 2012, ISBN: 978-3936931808
- Van Bon, Jan: Itil® 2011 Edition – Das Taschenbuch. Van Haren Publishing, 2012. ISBN: 978-9087537050
- Nadin Ebel: Basiswissen ITIL® 2011 Edition: Grundlagen und Know-how für das IT Service Management und die ITIL®-Foundation-Prüfung. dpunkt.verlag GmbH; 1. Auflage, 2014. ISBN: 978-3864901478

Netzwerksicherheit

Netzwerksicherheit: Client & Server			
Modulkürzel:	SPM-Netzwerksicherheit: Client & Server	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Netzwerksicherheit: Client & Server		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Grundlagen der Informatik, Einführung in die IT-Sicherheit		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden können Netzwerkgeräte (Switch, Router, Firewall, Wireless Access Points) konfigurieren. Sie sind in der Lage, die Mechanismen von TCP/IP für die Konfiguration von Endgeräten (Clients und Server) zu beschreiben und die Netzwerkkonfiguration zu automatisieren. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... Netzwerkgeräte zu konfigurieren. • ... Protokolle für die Kommunikation von Clients und Servern zu konfigurieren und zu optimieren. • ... Switching und Routing einzurichten. • ... komplexe Netzwerke aufzubauen. Handlungskompetenz: Die Studierende können ... • ... gängige Tätigkeiten der Netzwerkadministration ausführen. • ... Protokolle auf der Kontrollebene von Netzwerkgeräten zu nutzen.			

- ... moderne Ansätze wie Netzwerkvirtualisierung einsetzen.

Sozialkompetenz:

Die Studierenden können ...

- ... komplexe technische Problemstellungen aus dem Bereich Netzwerkadministration im Team erörtern.
- ... ihre Präsentationsfähigkeiten ausbauen.
- ... die Fähigkeit zum Zeitmanagement verbessern.

Inhalt:

- Konfiguration von Switchen, Routern und Wireless Access Points
- Absicherung von Client- & Serversystemen (insb. Windows & Linux)
- Grundlagen Public Key Infrastruktur (PKI) & Zertifikate
- Richtige Konfiguration von Firewalls, Einrichtung von VPNs
- Verschlüsselung der Dateiablage, z.B. Bitlocker, True-/VeraCrypt, etc.
- Intrusion Detection & Prevention Systeme, z.B. Snort, OSSEC, Security Onion, etc.
- Honey Pots & Co.

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Peter Kloeppel: PKI und CA in %0AWindows-Netzwerken: Das Handbuch für Administratoren. %0AZertifikat-Management und Sicherheit für Ihre Windows-Systeme, Rheinwerk Computing, 1. Auflage (27. Dezember 2017), ISBN: 978-3836255905
- Donald%0A A. Tevart: Mastering Linux Security and Hardening: Secure your Linux %0Aserver and protect it from intruders, malware attacks, and other %0Aexternal threats, Packt Publishing - ebooks Account (January 11, 2018), %0AISBN: 978-1788620307
- Kyle Rankin: Linux Hardening in Hostile %0ANetworks: Server Security from TLS to Tor, Addison-Wesley Professional, 1%0A edition (August 5, 2017), ISBN: 978-0134173269

Netzwerksicherheit: Analyse			
Modulkürzel:	SPM-Netzwerksicherheit: Analyse	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Netzwerksicherheit: Analyse		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Modul "Grundlagen der Informatik"		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die Protokolle des TCP/IP Netzwerkstacks im Detail. Sie sind in der Lage, die Mechanismen von TCP/IP und Ethernet zu beschreiben und Werkzeuge zur Netzwerkanalyse anzuwenden. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... die Protokolle des TCP/IP Stacks in ihrem Zusammenspiel zu verstehen. • ... Netzwerktopologien zu verstehen und Protokolle zu analysieren. • ... Schwachstellen in Netzwerken zu identifizieren. • ... Netzwerke abzusichern. Handlungskompetenz: Die Studierende können ... • ... Netzwerkprobleme und Applikationsprobleme unterscheiden. • ... Netzwerkanalysewerkzeuge einsetzen. • ... Fehler in TCP/IP Applikationen suchen.			

Sozialkompetenz: Die Studierenden können ... • ... komplexe technische Problemstellungen aus dem Bereich Netzwerksicherheit im Team erörtern. • ... ihre Präsentationsfähigkeiten ausbauen. • ... die Fähigkeit zum Zeitmanagement verbessern.
Inhalt:
• Vertiefte Grundlagen von Netzwerkprotokollen, insb. TCP/IP • Analyse von Netzwerktopologien, Auffinden von Schwachstellen • Analyse von Netzwerkprotokollen, Identifikation von Schwachstellen • Absicherung von Netzwerken / Netzwerkprotokollen • Vertiefung und Veranschaulichung der behandelten Themen in der Übung
Studien- / Prüfungsleistungen:
Studienarbeit (außerhalb Prüfungszeitraum) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • James Forshaw: Netzwerkprotokolle hacken: Sicherheitslücken verstehen, analysieren und schützen, dpunkt.verlag GmbH, 1. Auflage (25. Juni 2018), ISBN: 978-3864905698 • Laura Chappel: Wireshark® 101: Einführung in die Protokollanalyse, mitp Verlag, 2. Auflage 2018 (31. Januar 2018), ISBN: 978-3958456839 • Tim Philipp Schäfers: WLAN Hacking: Schwachstellen aufspüren, Angriffsmethoden kennen und das eigene Funknetz vor Hackern schützen. WLAN-Grundlagen und Verschlüsselungsmethoden erklärt, FRANZIS Verlag GmbH, 1. Auflage (15. Januar 2018), ISBN: 978-3645605236 • Steffen Wendzel: IT-Sicherheit für TCP/IP- und IoT-Netzwerke: Grundlagen, Konzepte, Protokolle, Härtung, Springer Vieweg Verlag, 1. Auflage 2018 (5. September 2018), ISBN: 978-3658226022 • Eric D. Knapp et al.: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Syngress Verlag, 2. Auflage (15. Dezember 2014), ISBN: 978-0124201149

2.5 Vertiefung/Erweiterung der Spezialisierungen

Biometrie: Deep Learning			
Modulkürzel:	VESPM-Biometrie: Deep Learning	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	Biometrie: Deep Learning		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach und Methodenkompetenz Die Studierenden verstehen die Grundprinzipien von Deep Learning Methoden, welche heutzutage weit verbreitet in der Künstliche Intelligenz sind, insbesondere für Muster Erkennung oder Biometrie. Sie werden sich nicht nur mit linearen Netzen arbeiten, sondern auch mit Convolutional Neural Networks (CNN) für Bildverarbeitung und Long Short-Term Memory (LSTM) Networks für die Verarbeitung von Sequenzen. Handlungskompetenz Die Studierenden können verschiedene Ansätze vergleichen, ihre Vorteile und Nachteile besprechen, und entscheiden, welches der beste Ansatz zur Bewältigung der anstehenden Herausforderungen ist.			
Inhalt:			
- Grundlagen der deep learning - Convolutional Neural Networks - Long Short-Term Memory (LSTM) Networks - Generative Adversarial Networks (GAN) und Autoencoders (AE) - Biometrische Erkennung und deep learning			

Angriffserkennung in der Biometrie: Presentation Attack Detection (PAD) und deep learning
Studien- / Prüfungsleistungen:
Schriftliche Prüfung, 90 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • I. Goodfellow, Y. Bengio, A. Courville: Deep Learning (Adaptive Computation and Machine Learning series), The MIT Press; Illustrated Edition (18. November 2016), ISBN: 978-0262035613 • F. Chollet: Deep Learning with Python, Manning Publications, 2017, ISBN: 978-1617294433 • B. Bhanu, A. Kumar: Deep Learning for Biometrics, Springer, 2017, ISBN: 978-3319616568 Forschungsartikel in peer-reviewed Konferenzen oder Journalen

IT-Collaboration und Integration			
Modulkürzel:	VESPM-IT-Collaboration und Integration	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	4	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Sommersemester		
Lehrveranstaltungen des Moduls:	IT-Collaboration und Integration		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS/WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden kennen die typischen Anforderungen an Lösungen zur IT-Collaboration und die damit einhergehenden datenschutzrechtlichen und sicherheitstechnischen Fragestellungen in kleinerer bis mittlerer Unternehmen. Die Studierenden haben erste praktische Erfahrungen mit der Einrichtung, Konfiguration und dem Betrieb einer modernen Software zur Unterstützung von Arbeitsabläufen in Teams gesammelt. Die Studierenden kennen die wichtigsten datenschutzrechtlichen Rahmenbedingungen, sowie technische Grundlagen für die Sicherstellung des technischen Datenschutzes kleinerer bis mittlerer Organisationen. Handlungskompetenz: Die Studierenden können im Unternehmen aktiv an der Entwicklung einer IT-gestützten Kollaborationslösung mitarbeiten. Sie besitzen die Fähigkeit eine moderne IT-Collaboration-Software in kleinen bis mittleren Unternehmen, insb. auch unter datenschutzbezogenen Aspekten, zu planen, einzurichten und zu betreiben. Die Studierenden sind fähig an Konzeption und Aufbau einer sicheren Netzwerk- und Systeminfrastruktur aktiv mitzuwirken und einfache Konfigurationsaufgaben selbständig zu übernehmen. Sozialkompetenz: Die Studierenden sind in der Lage die Vorteile der IT-Unterstützung von Arbeitsabläufen typischer InformationWorker zu vermitteln und können die Anwender schrittweise an dieses neue Werkzeug heranführen. Die Studierenden können Anwendern verständlich vermitteln warum bestimmte technische,			

organisatorische und datenschutzrechtliche Maßnahmen notwendig sind um die IT-Sicherheit im Unternehmen zu gewährleisten.
Inhalt:
Die Lehrveranstaltung ist eine Kombination zweier eigenständiger Teile, die in der Praxis oft Hand in Hand gehen: Die Unterstützung der Zusammenarbeit von Information-Workern im Unternehmen und der sichere Aufbau und Betrieb von Netzwerken in kleineren bis mittleren Organisationen. Unter anderem werden die folgenden Themen behandelt: • Web Content Management (WCM) / Records Management • Workflow Management (WfM)/ Business Process Management (BPM) • Document Management (DM) • Microsoft SharePoint Online und SharePoint Server • Ausgewählte Grundlagen des Datenschutzrechts und rechtliche Anforderungen an Unternehmen • Sicherheitsaspekte von Netzwerkinfrastrukturen und ausgewählte Angriffsvektoren
Studien- / Prüfungsleistungen:
mündliche Prüfung, 20 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Lanphier, Troy: "Managing Microsoft SharePoint Server 2016 ", Microsoft Press, 2016, ISBN: 978-1509302949 • Andrew S. Tanenbaum; David J. Wetherall: "Computernetzwerke", Pearson Studium, 5. Auflage, 2012, ISBN: 978-3866451568 • Kranig, Thomas; Sachs, Andreas; Gierschmann, Markus: Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden, Bundesanzeiger; 1. Auflage, 2017, ISBN: 978-3846207604 • Petric, Ronald, et al.: "Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie", Springer Vieweg; 1. Auflage, 2017, ISBN: 978-3658168384

2.6 Fachspezifisches Wahlpflichtmodul

Design Thinking			
Modulkürzel:	DIS-Design Thinking	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):			
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Design Thinking		
Lehrformen des Moduls:	Präsenz oder Blended-Learning bzw. online – Achtung: Wir streben ggw. eine wöchentlich stattfindende Präsenzveranstaltung an. Aufgrund Corona findet diese Veranstaltung möglicherweise kurzfristig im e-Learning-Modus, ggf. auch in Form von 5 ganztägigen Online-Präsenzseminaren statt. Bitte beachten Sie diesbezüglich die Hinweise auf Moodle! Kurzfristige Umstellung auch einzelner Veranstaltungen von offline auf online sind möglich.		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Design Thinking ist eine kreative, empathische Methode zur Konzeptentwicklung, die sich im IT- sowie im betriebswirtschaftlichen Bereich nach wie vor stetig zunehmender Beliebtheit erfreut. Sie gilt mittlerweile als Schlüsselkompetenz, die auch und gerade im Kontext der Digitalen Transformation gefragt ist und von vielen Unternehmen gefordert wird. In diesem Modul werden Ihnen die entsprechenden Kenntnisse in dieser Methode vermittelt. Im Modul werden praxisnahe Fragestellungen bearbeitet. Fach- und Methodenkompetenz Kenntnis der wesentlichen Aspekte von Design Thinking. Handlungskompetenz: Fähigkeit zur Anwendung von Design Thinking in und für den Projekt- und Unternehmenskontext. Fähigkeit zur Recherche relevanten Wissens aus der Literatur. Eigenständiger Erwerb von relevantem Fach- und Kontextwissen.			

Sozialkompetenz: Entwicklung von Sozialkompetenz durch Design Thinking, insbesondere Führungskompetenzen, Teamfähigkeit und Kommunikationsfähigkeit sowie Empathie mit Kunden und Nutzern.
Inhalt:
Die Inhalte der Veranstaltung umfassen die Vermittlung von Kenntnissen rund um Design Thinking sowie deren praktische Anwendung. Es wird viel im Team gearbeitet. Im Rahmen des Moduls werden Aufgaben aus realen bzw. realitätsnahen Fällen erarbeitet bzw. simuliert. Auf fortgeschrittene und aktuelle Themen im Kontext der Methode wird eingegangen.
Studien- / Prüfungsleistungen:
mündliche Prüfung, 15 Minuten (elektronische Fernprüfung nach § 2 Abs. 3 BayFEV) Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.
Literatur: • Uebernicket, Brenner, Pukall, Naef, Schindlholzer (2015) Design Thinking – Das Handbuch, Frankfurter Allgemeine Buch • Lewrick, Link, Leifer (2020) Das Design Thinking Toolbook: Die besten Werkzeuge und Methoden, Vahlen

Sicherh. und Datensch. mit verrauschten Daten			
Modulkürzel:	DIS-Sich. und Datensch. mit verr. Daten	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Marta Gomez-Barrero		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Sicherh. und Datensch. mit verrauschten Daten		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden lernen, wie man mit verrauschten Daten bzgl. Sicherheit und Datenschutz arbeiten kann. Verschiedene Werkzeuge werden beschrieben, um das Sicherheitsziel Vertraulichkeit mit solchen Daten gewährleisten zu können. Besondere relevante Fallstudien in der Wirtschaft mit biometrischen Daten und Physically Unclonable Functions werden dabei helfen, die neuen Werkzeuge zu beherrschen. Dabei erweitern die Studierenden ihre Kompetenz spezifische Technologien auszuwählen und in einem konkreten Projekt zu implementieren. Handlungskompetenz Die Studierenden vertiefen die Kompetenz mit mehreren spezifischen kryptographischen Methoden umzugehen. Sie sind in der Lage, die Herausforderungen an den Datenschutz und die Sicherheit zu verstehen, die durch verrauschte Daten entstehen, und sie können geeignete kryptographische Werkzeuge zum Schutz der Daten wählen.			

Inhalt:
• Grundlagen der Sicherheit mit verrauschten Daten • Fuzzy commitment, Fuzzy extractors und Error Correcting Codes (ECC) • Homomorphe Verschlüsselung • Multi-Party Computation • Anwendungen: Biometric Template Protection und Physically Unclonable Functions (PUFs) • ISO/IEC Standards 24745 und 30136
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • P. Tuyls, B. Škoric, T. Kevenaar: Security with Noisy Data: on private biometrics, secure key storage and anti-counterfeiting, Springer Science & Business Media, 2007. ISBN: 978-1-84628-983-5 • P. Campisi: Security and privacy in biometrics, Springer, 2013. ISBN: 978-1-4471-6201-8 • E. J. Kindt: Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis, Springer, 2016. ISBN: 978-94-024-0647-4 • C. Böhm, M. Hofer: Physically Unclonable Functions in Theory and Practice, Springer Science & Business Media, 2012. ISBN: 978-1-4939-4498-9

Urheberrecht			
Modulkürzel:	DIS-Urheberrecht	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Stefanie Fehr		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Urheberrecht		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Die Studierenden kennen die Entstehungsgeschichte und die ökonomische Bedeutung des Urheberrechts. Die besondere Herausforderung, welche die Digitaltechnik für das Urheberrecht darstellt, ist ihnen bewusst. Sie verfügen über Kenntnisse des materiellen Urheberrechts, seiner verfahrensrechtlichen Regelungen sowie seiner europäischen und internationalen Wurzeln und können urheberrechtliche Fälle lösen. Letzteres wird durch praxisnahe Übungen gefestigt. Fach- und Methodenkompetenz: Die Studierenden werden befähigt ... • ... den Anwendungsbereich des Urheberrechts zu definieren. • ... zwischen dem Urheberrecht und anderen Immaterialgüterrechten zu unterscheiden. • ... die Grundzüge des Urheberrechts und seiner Bedeutung für den Wirtschafts- und Rechtsverkehr in der Informationsgesellschaft zu benennen. • ... einfache Sachverhalte im Urheberrecht methodisch zu prüfen. • ... aktueller und praxisrelevanter Diskussionen aus dem Bereich des Urheberrechts zu folgen. Handlungskompetenz: Die Studierenden können ... • ... im Anwendungsfall Sachverhalte dem Urheberrecht zu ordnen und Handlungsoptionen ableiten. • ... die Schranken des Urheberrechts bestimmen. Sozialkompetenz: Die Studierenden können ...			

• ... einfache Sachverhalte im Kontext des Urheberrechts methodisch prüfen und anwenden. • ... aktueller und praxisrelevanter Diskussionen aus dem Bereich des Urheberrechts folgen.
Inhalt:
• Entstehungsgeschichte und (Schutz-)Zwecke des Urheberrechts • Einbettung des Urheberrechts in den europäischen Kontext • Abgrenzung Urheberrecht zum Datenschutzrecht • materielles Urheberrecht (einschließlich der verwandten Schutzrechte), insbesondere Verwertungsrechte und Schranken • Urhebervertragsrecht und Grundzüge des Urhebervertragsrechts
Studien- / Prüfungsleistungen:
schriftliche Prüfung, 90 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Literatur: • Rehbinder, M., Peukert, A. (2018): Urheberrecht. • Pierson, M., Ahrens, T., Fischer, K. (2018): Recht des geistigen Eigentums. • Lutz, P. (2018): Grundriss des Urheberrechts. • Schwartmann, R. (2017): Praxishandbuch Medien-, IT- und Urheberrecht. • Schwartmann, R., Hentsch, C. (2016): Falltraining im Urheberrecht.

Virtualisierungs- und Containertechniken			
Modulkürzel:	WIF-Virtualisierungs- und Containertechniken	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	5	
Modulverantwortliche(r):	Prof. Dr. Jens-Henrik Söldner		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Virtualisierungs- und Containertechniken		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Die Teilnahme an Prüfungen der Modulgruppen Spezialisierungen (SPM), Vertiefung oder Erweiterung der Spezialisierungen (VESPM) und fachspezifische Wahlpflichtmodule (FWPM) ist nur möglich, wenn alle Module des ersten Fachsemesters bestanden sind		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden erhalten einen umfassenden Überblick über moderne Arten der Bereitstellung von Compute-Workloads - virtuelle Maschinen und Container. Sie erlernen, wie komplexe Infrastrukturen zur Bereitstellung von virtuellen Maschinen und Containern aufgesetzt, administriert, gewartet und genutzt werden können. Handlungskompetenz: Die Studierenden können fachliche Entscheidungen in den behandelten Bereichen selbständig treffen. Sie besitzen zudem die Fähigkeit, sich eigenständig in Fachgebiete zielgerichtet einzuarbeiten und die dazu notwendigen Informationen zu beschaffen. Die Studierenden können bei der Auswahl von Virtualisierungs- und Containerinfrastrukturen aktiv mitwirken, um den operativen Betrieb dieser Techniken in Organisationen möglichst effizient zu gestalten. Sozialkompetenz: Aufbauend auf Ihren Erfahrungen in der Lehrveranstaltung besitzen die Studierenden die Fähigkeit, Fachprobleme in Kleingruppen zu diskutieren und eigene Lösungsvorschläge im Kollegenkreis zielgerichtet zu vermitteln.			

Inhalt:

- Geschichte der Virtualisierung und Containerisierung
- Typen von Hypervisoren
- Arten der Virtualisierung: Servervirtualisierung, Speichervirtualisierung, Netzwerkvirtualisierung, Desktopvirtualisierung
- Erstellen von virtuellen Maschinen und Containern
- Grundlagen von Firmennetzen für die Architektur von Virtualisierungs- und Containersysteme: VLAN-Segmentierung, Routing, Layer 2 und Layer 3 Switches, Overlay-Protokolle
- Einbindung von virtuellen Maschinen und Containern in Netzwerkinfrastrukturen
- Exkurs Speichersysteme: Fibre Channel, iSCSI, NFS, Block vs File, Hyperconverged Storage
- Cluster- und Hochverfügbarkeitstechniken
- Sicherheit von Virtualisierungsinfrastrukturen
- Container: Ausblick auf Kubernetes

Studien- / Prüfungsleistungen:

mündliche Prüfung, 15 Minuten

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

- Bertram Wöhrmann et al.: VMware vSphere 7 - Das umfassende Handbuch, 6. aktualisierte und erweiterte Auflage (2020), Verlag Rheinwerk Computing, ISBN: 978-3-8362-7578-1
- Michael Kofler et al.: Hacking & Security: Das umfassende Handbuch, 1. Auflage (27. April 2018), Verlag Rheinwerk Computing, ISBN: 978-3836245487
- Online-Materialien der VMware IT Academy
- Online-Materialien der Red Hat IT Academy
- aktuelle Artikel aus Fachzeitschriften (iX, IT Administrator)

2.7 Allgemeine Wahlpflichtmodule

Controlling & Business Leadership			
Modulkürzel:	Contr. & Bus. Lead.	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Michael Müller		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Controlling & Business Leadership		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach – und Methodenkompetenz:			
- Anwendung von theoretischem Wissen in der Praxis - Methoden des Financial Controlling und der Unternehmensführung eines international operierenden Unternehmens basierend auf praktischen Beispielen - Die Englisch basierende Vorlesung (englische Unterrichtssprache, englisches Script) vermittelt internationale Unternehmenskultur			
Handlungskompetenz:			
Das Ziel wird über ein aufgaben- und ergebnisorientiertes learning by doing bzw. learning through interaction – in Partner- oder Gruppenarbeit – angegangen			
Sozialkompetenz:			
- Die unterschiedlichen und vielfältigen Fallstudien werden in Partner – und Gruppenübungen durchgeführt . - Diese Aktivitäten führen zum gruppenspezifischen Arbeiten, teambuilding, Präsentation innerhalb und für die Gruppe, etc)			

Inhalt:
• Introduction • Financial Awareness Training for all Employees • Deployment of the Company's Strategy and Goals • KPI's - Key Performance Indicators (TMC, MOE, Productivity, Process Reliability, Scrap etc) • Balanced Scorecard as tool for Business Leadership • Budget Planning – TMC (Total Manufacturing Costs) • Business Review (actual results) – Monthly TMC Analysis • Importance of Working Capital and Inventories • NPV – Net Present Value as instrument for Capital Investment and strategic decision making • Special Topic: „Controlling in growing digitization“ • Business Decision Making supported by Financial Analysis (example) • Wrap up
Studien- / Prüfungsleistungen:
Schriftliche Prüfung, 90 Minuten Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan. Vorlesungsscript

Datenbanken			
Modulkürzel:	DIS-Datenbanken	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Bernhard Volz		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Datenbanken		
Lehrformen des Moduls:	DIS + WIF		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	DIS + WIF		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz Die Studierenden ☐ kennen Sinn und Gründe für den Datenbanksystem(DBS)-Einsatz ☐ können konzeptuelle Datenmodelle erstellen (semantische Modellierung) – insbesondere Entity-Relationship-Modelle (ERM) - und diese in logische Datenmodelle transformieren – insbesondere in das relationale, ☐ kennen die Normalformentheorie und ihre Anwendung, ☐ können Standard SQL und Datendefinitions- bzw. Datenmanipulationssprachen ausgewählter Datenbanksysteme anwenden, ☐ kennen die Konzepte und Mittel der Datenbankanwendungsprogrammierung, ☐ kennen die Anwendungsbereiche und Architektur objektorientierter und objektrelationaler Datenbanken, ☐ kennen wichtige Administrationsmethoden von Datenbanksystemen. Handlungskompetenz Die Studierenden können für typische betriebliche Aufgabenstellungen ein Datenbanksystem entwerfen, einrichten und die für den Endbenutzer notwendigen Funktionen bereitstellen/implementieren – auch unter dem Aspekt der Mehrbenutzersynchronisation.			
Inhalt:			
☐ Einführung in relationale Datenbanken: Architektur, Drei-Ebenen- Konzept nach ANSI/SPARC, Gegenüberstellung traditioneller und moderner, semantischer und logischer Datenbankmodelle ☐ Modellierung, Design und Implementierung: ERM, Normalformen und Designfragen relationaler Datenbanken, Sprachklassen, Structured Query Language (SQL)			

☐ Datenbankprogrammierung: Embedded SQL mit Java und c#, Java Database Connectivity (JDBC), Datenbankprozeduren, O/R-Mapping: Abbildung von Klassen auf Datenbanktabellen und umgekehrt; Trigger und Transaktionen

☐ Einführung in die Datenbankadministration: Datenbank-, Nutzer-, und Rechteverwaltung, Backup und Recovery, Sicherheitskonzepte

Studien- / Prüfungsleistungen:

schriftliche Prüfung, 90 Minuten (elektronische Fernprüfung nach § 2 Abs. 1 BayFEV)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

☐ Heuer, G. Saake, K.-U. Sattler: Datenbanken kompakt, mitp

☐ Heuer, G. Saake, K.-U. Sattler: Datenbanken Konzepte und Sprachen, mitp

☐ Kemper, A. Eickler: Datenbanksysteme – Eine Einführung, Oldenbourg Verlag

☐ G. Vossen: Datenmodelle, Datenbanksprachen und Datenbankmanagementsysteme, Oldenbourg Verlag

☐ Webcast und Online-/Video-Tutorials laut aktueller Empfehlung

☐ R. A. Elmasri, S.B. Navathe: Grundlagen von Datenbanksystemen – Bachelorausgabe, Pearson Studium

Spanisch 1 (für Anfänger) (P)3

Modulkürzel:	Spanisch 1 (für Anfänger) (P)3	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Dr. Christian Gebhard		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Spanisch 1 (für Anfänger) (P)3		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Interesse an spanischsprachigen Kulturen Teilnahmevoraussetzungen gem. SPO:		
Verwendbarkeit:	DIS		
Angestrebte Lernergebnisse:			
Fach- und Methodenkompetenz: Die Studierenden besitzen Grundkenntnisse in Lexik, Morphologie, Syntax und Pragmatik. Handlungskompetenz: Die Studierenden sind in der Lage, einfache Situationen des Alltagslebens kommunikativ zu bewältigen. Sozialkompetenz: Teamfähigkeit und Kommunikationsfähigkeit, angemessenes Bitten um Hilfe im kommunikativen Prozess.			
Inhalt:			
Im Modul werden Grundlagen der Sprachverwendung und landeskundliche Kenntnisse vermittelt. Das Modul besteht aus seminaristischem Unterricht mit aktivem Charakter. Die vier Grundfertigkeiten Hörverständnis, mündlicher Ausdruck, Leseverständnis und schriftlicher Ausdruck werden mit Fokus auf mündlichen Ausdruck und Lese- und Hörverständnis grundlegend vermittelt. Alltagssituationen stehen inhaltlich im Mittelpunkt (Vorstellen, Auskünfte einholen und Auskünfte geben v.a. beim Einkaufen und Wegbeschreibungen, allgemeine Konversation). An grammatikalischen Erscheinungen werden mindestens durchgenommen: - Ausspracheregeln und Grundregeln der Orthographie - Konkordanz (zwischen Subjekt und Verb, Substantiv und Adjektiv)			

- Personal-, Demonstrativ-, Possessiv- und Fragepronomen (einführend)
- Verwendung von direkten und indirekten Objekten (einführend)
- Verlaufsform
- Regelmäßige und unregelmäßige Verben (Vokalveränderung) im Präsens
- Perfecto
- Periphrastische Strukturen (einführend)
- Komparativ und Superlativ (einführend)
- Imperativ (einführend)

Studien- / Prüfungsleistungen:

Studienarbeit (außerhalb Prüfungszeitraum)

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

Universo.ele A1. Hueber. Kursbuch + Arbeitsbuch + CD: 978-3-19-004333-0

Unternehmensberatung			
Modulkürzel:	DIS-Unternehmensberatung	Modul-Nr.:	
Zuordnung zum Curriculum:	Studiengang u. -richtung	Studiensemester	
	Datenschutz und IT-Sicherheit (SPO WS 21/22)	3	
Modulverantwortliche(r):	Prof. Dr. Bernd Heesen		
Sprache:	Deutsch		
Leistungspunkte / SWS:	5 ECTS / 4 SWS		
Arbeitsaufwand:	Kontaktstunden:	45 h	
	Selbststudium:	105 h	
	Gesamtaufwand:	150 h	
Moduldauer:	1 Semester		
Häufigkeit:	nur Wintersemester		
Lehrveranstaltungen des Moduls:	Unternehmensberatung		
Lehrformen des Moduls:	SU/Ü - seminaristischer Unterricht/Übung		
Teilnahmevoraussetzung:	Keine		
Empfohlene Voraussetzungen:	Keine		
Verwendbarkeit:	Keine		
Angestrebte Lernergebnisse:			
Fach-und Methodenkompetenz Die Studierenden bekommen einen wesentlichen Einblick in Marktstrukturen, Trends & Entwicklungen der IT-und Managementberatungen. Des Weiteren erlernen sie die verschiedenen Perspektiven der Unternehmensberatung. Handlungskompetenz Die Studierenden können sowohl die Tätigkeiten als auch die Rolle eines Unternehmensberaters wahrnehmen. Sozialkompetenz Teamfähigkeit / Kommunikationsfähigkeit / Verhandlungsfähigkeit Zielorientierte, gruppenbezogene Erarbeitung von Case Studies mit anschließende Gruppenpräsentationen / -Diskussionen			
Inhalt:			
-Aktuelle Marktstudien der IT-und Managementberatungen in Deutschland -Case Study „Running a Consulting Company“ -Einblick in die Unternehmensberatung (Descriptive, Practitioner, Critical & Career Perspective) -Case Study „Beratungsprojekt“			
Studien- / Prüfungsleistungen:			
mündliche Prüfung, 30 Minuten (elektronische Fernprüfung nach § 2 Abs. 3 BayFEV)			

Voraussetzungen für die Vergabe von Leistungspunkten, ist das Bestehen der jeweiligen Modulprüfung gem. SPO bzw. Studienplan.

Literatur:

-O'Mahoney, J. & Markham, C. (2013). Management Consultancy. Oxford University Press. ISBN: 978-0-19-964547-3.

-Lünendonk Studien (frei zugänglich)

-Staufenbiel Institut Studien (frei zugänglich)