Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT Security an der Universität zu Lübeck mit dem Abschluss „Master of Science"

Vom 31. Januar 2017 (NBl. HS MSGWG Schl.-H. S. 35)

geändert durch:
Satzung vom 4. Juli 2019 (NBl. HS MBWK Schl.-H. S. 50)
Satzung vom 15. Februar 2022 (NBl. HS MBWK Schl.-H. S. 31)

§ 1
Geltungsbereich

Diese Studiengangsordnung regelt in Verbindung mit der Prüfungsverfahrensordnung (PVO) der Universität zu Lübeck für Studierende der Bachelor- und Masterstudiengänge das Masterstudium IT Security an der Universität zu Lübeck.

§ 2
Studienziel

(1) Das Masterstudium bereitet die Absolventinnen und Absolventen auf Tätigkeiten im Bereich der IT-Sicherheit und Zuverlässigkeit in forschungs-, lehr-, entwicklungs- und anwendungsbezogenen Berufsfeldern vor.

(2) Das Ziel des Masterstudiengangs IT Security besteht darin, die Studierenden durch Vermittlung von wissenschaftlichen Methoden und Modellen sowie Einübung von Fertigkeiten der IT-Sicherheit und Zuverlässigkeit in die Lage zu versetzen, vielfältige Probleme der sicheren und zuverlässigen Informationsverarbeitung zu verstehen und zu bearbeiten. Gegenstand des Studiengangs ist die Analyse, Beschreibung, Konstruktion und Validierung von informationsverarbeitenden Systemen, insbesondere unter dem Aspekt der Sicherheit und Zuverlässigkeit. Dabei liegt im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für wissenschaftliches Arbeiten. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung und soll die Voraussetzung für ein lebenslanges Lernen im Bereich der Informatik und spezieller der sicheren und zuverlässigen IT-Systeme sowie für eine weitergehende akademische Qualifikation z.B. die Promotion schaffen. Weiterhin sollen die Studierenden aufgrund der

von ihnen erworbenen Kompetenzen in der Lage sein, Leitungsfunktionen in der Wirtschaft zu übernehmen.

(3) Der Masterstudiengang IT Security ist forschungsorientiert und konsekutiv zum Bachelorstudiengang IT-Sicherheit der Universität zu Lübeck aufgebaut. Von den Studierenden wird als Voraussetzung erwartet, dass sie bereits Wissen, Fertigkeiten und Kompetenzen im Bereich der IT-Sicherheit und Zuverlässigkeit in Umfang und Tiefe besitzen, wie es im Bachelorstudiengang vermittelt wird.

(4) Bei erfolgreichem Abschluss des Masterstudiums verleiht die Universität zu Lübeck den akademischen Grad „Master of Science".

§ 3
Zugang zum Studium

(1) Der Masterstudiengang ist konsekutiv zum Bachelorstudiengang IT-Sicherheit der Universität zu Lübeck.

(2) Voraussetzung für den Zugang zum Masterstudiengang IT Security ist, dass die Bewerberin oder der Bewerber folgende Nachweise erbringt:

1. Bachelorabschluss in IT-Sicherheit oder einem verwandten Fach, wofür die Bewerberin oder der Bewerber nachweisen muss,
   a) dass sie oder er einen Bachelorabschluss oder einen diesem gleichwertigen Abschluss im Studiengang IT-Sicherheit oder in einem fachlich eng verwandten Studiengang an einer deutschen Hochschule oder an einer Hochschule erworben hat, die einem der Bologna-Signatarstaaten angehört oder
   b) dass sie oder er an einer ausländischen Hochschule einen gleichwertigen Abschluss in einem fachlich eng verwandten Studiengang erworben hat.

   Die Gleichwertigkeit eines ausländischen Abschlusses wird nach Maßgabe der Bewertungsvorschläge der Zentralstelle für ausländisches Bildungswesen beim Ständigen Sekretariat der Kultusministerkonferenz festgestellt. Die Noten der ausländischen Bildungsnachweise sind in das deutsche Notensystem umzurechnen.
2. Besondere Qualifikation
   a) Erststudium mit einer Note von 2,7 oder besser abgeschlossen.
   b) der Umfang der grundlegenden, mathematischen Konzepte der Stochastik, Analysis und Linearen Algebra in dem von der Bewerberin oder dem Bewerber absolvierten Bachelorstudium muss mindestens 28 Kreditpunkte (KP) betragen haben.
   c) der Umfang der grundlegenden informatischen Anteile wie Softwareentwicklung, IT-Sicherheit, Kryptologie, Rechnersysteme und theoretische Informatik in dem von der Bewerberin oder dem Bewerber absolvierten Bachelorstudium muss mindestens 60 KP betragen haben.
   d) mindestens 12 KP davon aus dem Bereich der IT-Sicherheit.

e) Im Einzelfall kann von den Vorgaben a) - d) abgesehen werden, wenn die Bewerberin oder der Bewerber ihre oder seine fachliche Eignung auf andere geeignete Art und Weise nachweist.

3. Ausreichende Kenntnisse der englischen Sprache gemäß CEFR B2 (nachzuweisen durch ein deutsches Abiturzeugnis, nach dem die Sprache für mindestens sieben Jahre belegt wurde oder durch entsprechende Sprachprüfungen (z.B. TOEFL, IELTS)).

(3) Über das Vorliegen und die Erfüllung der in Absatz 2 genannten Zugangsvoraussetzungen entscheidet der Prüfungsausschuss.

(4) Wenn zum Bewerbungszeitpunkt das qualifizierende Studium noch nicht abgeschlossen ist, die Bachelorarbeit aber bereits begonnen wurde, genügt der Nachweis von Prüfungsleistungen im Umfang von mindestens 135 Kreditpunkten und eine aus diesen Prüfungsleistungen ermittelte Durchschnittsnote von mindestens 2,7, um unter Vorbehalt zugelassen zu werden. In diesem Fall ist der erfolgreiche Studienabschluss innerhalb von drei Monaten nach Studienbeginn nachzuweisen. Geschieht dies nicht, so erlischt die Zulassung.

(5) Die Einschreibung ist zu versagen, wenn die Bewerberin oder der Bewerber eine nach einer Prüfungsordnung im Studiengang IT-Sicherheit erforderliche Prüfung an einer Hochschule in Deutschland endgültig nicht bestanden hat oder wenn sie oder er sich in solch einem Studiengang in einem Prüfungsverfahren befindet.

(6) Das Studium kann zum Sommer- und zum Wintersemester aufgenommen werden.

§ 4
Master Agreement

Bei Bewerberinnen und Bewerbern, bei denen der Prüfungsausschuss aufgrund deren im Bachelorstudium erworbenen Kompetenzen die Nachholung von fachlichen Voraussetzungen aus dem Bachelorstudiengang für sachlich sinnvoll erachtet, kann zwischen der oder dem Studierenden und der oder dem Prüfungsausschussvorsitzenden ein sog. Master Agreement abgeschlossen werden. In diesem wird vereinbart, welche Module aus dem Bachelorstudium bis zu welchem Zeitpunkt erfolgreich absolviert werden sollten. Es dürfen nicht mehr als drei Module vereinbart werden. Bei Verfehlen der vereinbarten Modulabsolvierung lädt die oder der Prüfungsausschussvorsitzende zu einer Studienberatung gemäß § 6 PVO ein.

§ 5
Studieninhalte

Das Studium gliedert sich in folgende Teilbereiche:

1. Erwerb von Kenntnissen und Fähigkeiten im Bereich der theoretischen, praktischen und technischen Informatik einschließlich der Softwareentwicklung
2. Erwerb von tiefergehenden Kenntnissen in der IT-Sicherheit und Zuverlässigkeit
3. Fachspezifische Vertiefung durch Wahl weiterer Lehrmodule
4. Erwerb von fachübergreifenden Kompetenzen

§ 6
Struktur und Umfang des Studiums

(1) Das Studium umfasst Lehrveranstaltungen mit einem Gesamtumfang von 120 KP gemäß dem ECTS-Standard mit einer Regelstudienzeit von zwei Jahren. Der Umfang der Lehrmodule beträgt:

- im Pflichtbereich IT-Sicherheit 10 KP
- im Wahlpflichtbereich IT-Sicherheit 40 KP
- im Pflichtbereich Informatik 12 KP
- im Wahlpflichtbereich Informatik 12 KP
- im freien Vertiefungsbereich 12 KP
- im fächerübergreifenden Bereich 4 KP

Die Masterarbeit hat einen Umfang von 30 KP, ihr folgt ein abschließendes Kolloquium.

(2) Die Teilnahme an weiteren von der Universität angebotenen Lehrmodulen laut Modulhandbuch über den in Absatz 1 vorgegebenen Rahmen hinaus ist möglich und wird empfohlen. Derartige Prüfungsleistungen können auf Antrag im Diploma-Supplement aufgelistet werden, sofern sie im Modulhandbuch geführt sind.

(3) Die Lehrmodule der einzelnen Bereiche und die Wahlmöglichkeiten sind im Anhang aufgeführt und im Modulhandbuch detailliert beschrieben. Pflicht- und Wahlpflichtmodule, die bereits im vorangegangenen Bachelorstudium curricular vorgesehen sind und erfolgreich absolviert wurden, sind von einer Wahl im Masterstudiengang ausgeschlossen.

(4) Die Unterrichts- und Prüfungssprache ist Englisch. Innerhalb von Wahlpflichtmodulen können Veranstaltungen auch auf Deutsch durchgeführt werden, wobei jedoch immer eine englischsprachige Alternative angeboten wird.

§ 7
Masterprüfung und Prüfungsvorleistungen

(1) Die Masterprüfung besteht aus studienbegleitenden Fachprüfungen für die einzelnen Lehrmodule und der Masterarbeit mit einem abschließenden Kolloquium. Für Module der Kategorie A und B gemäß Anlage ist eine Prüfungsleistung gemäß § 12 Absatz 1 in Verbindung mit §§ 13 ff. PVO zu erbringen.

(2) Der Antrag auf Zulassung zur Masterarbeit ist gemäß § 11 Absatz 5 PVO gesondert schriftlich bei der oder dem Vorsitzenden des Prüfungsausschusses zu stellen.

(3) Die Zulassung zu den studienbegleitenden Fachprüfungen erfolgt gemäß § 11 PVO grundsätzlich mit der Einschreibung zum Masterstudiengang IT Security. Für die Zulassung zu einer Fachprüfung können gemäß § 11 Absatz 2 PVO Prüfungsvorleistungen definiert werden, die im Modulhandbuch vor Beginn des jeweiligen Moduls aufzuführen sind. Prüfungsvorleistungen sind vor dem Zeitpunkt der Prüfung abzuschließen und nachzuweisen und gehen nicht in die Modulnote ein.

§ 8
Fachliche Zulassungsvoraussetzungen für die Masterarbeit

Zur Masterarbeit kann nur zugelassen werden, wer die Voraussetzungen gemäß § 11 PVO erfüllt, sich mindestens im 3. Fachsemester befindet und Leistungszertifikate des Studiengangs im Umfang von mindestens 70 Kreditpunkten entsprechend § 6 Absatz 1 vorweist.

Anhang 1 zur Studiengangsordnung für den
Masterstudiengang IT Security
der Universität zu Lübeck
Die Modulkataloge

1. Vorbemerkung

In den folgenden Tabellen werden die Lehrmodule (LM) aufgelistet, für die Leistungszertifikate (LZF) zum Bestehen der Masterprüfung erworben werden müssen, unterteilt in die verschiedenen Studienbereiche. Für jedes Lehrmodul ist der Umfang der durchschnittlichen Präsenzstunden pro Woche (SWS), die Art – Vorlesung (V), Übung (Ü), Praktikum (P) oder Seminar (S) – die Anzahl der Kreditpunkte (KP) entsprechend dem European Credit Transfer System und der Typ des Leistungszertifikats – Kategorie A oder B – angegeben. Weitere Details wie Lernziele und Inhalte, die zu erbringenden Studienleistungen oder Art der Prüfung werden im Modulhandbuch (MHB) beschrieben.

2. Allgemeine Hinweise und Regeln bei der Wahl von Lehrmodulen

Die Studierenden können unter Beachtung der prüfungsrechtlichen Vorgaben Lehrmodule in den Wahlpflichtbereichen frei wählen. Dabei sind die folgenden Regeln zu beachten:

- Lehrmodule können nicht mehrfach angerechnet werden.
- Lehrmodule, die bereits im Prüfungszeugnis oder Diploma-Supplement des qualifizierenden Bachelor-Studiengangs aufgeführt sind, können nicht gewählt werden.
- Weitere Lehrmodule oder Modulkombinationen können auf begründeten Antrag vom Prüfungsausschuss genehmigt werden.
- Von den Wahlpflichtveranstaltungen wird in jedem Studienjahr nur eine beschränkte Anzahl von Lehrmodule und auch nur bei hinreichender Nachfrage realisiert.

3. Pflicht-Lehrmodule aus dem Bereich IT-Sicherheit

Modulnr.	**Pflicht-Lehrmodule IT-Sicherheit**	**SWS**	**KP**	**Typ LZF**
CS4701-KP06	Communication and System Security	2V+1Ü+1S	6	A
CS5195-KP04	Current Topics in IT Security	2V+1P	4	A
	Summe		**10**	

4. Wahlpflichtbereich IT-Sicherheit

Aus den folgenden zwei Wahlbereichen müssen jeweils zwei Module gewählt werden.

Modulnr.	**Themenbereich Security und Privacy**	**SWS**	**KP**	**Typ LZF**
CS4210-KP06	Cryptographic Protocols	3V+2Ü	6	A
CS4211-KP06	Modeling and Analysing Security	3V+1Ü+1P	6	A

CS4450-KP06	Networks and Mobile Systems	2V+2Ü	6	A
CS4451-KP06	Privacy	2V+2Ü	6	A
CS4702-KP06	Computer Security	2V+3P	6	A
	Zu erreichende Summe		**12**	

Modulnr.	**Themenbereich Safety und Reliability**	**SWS**	**KP**	**Typ LZF**
CS4138-KP06	Model Checking	3V+1Ü	6	A
CS4139-KP06	Runtime Verification and Testing	3V+1Ü	6	A
CS5220-KP06	Static Analysis	3V+1Ü	6	A
CS4452-KP06	Technische Reliability Engineering	2V+2Ü	6	A
	Zu erreichende Summe		**12**	

Im Wahlpflichtbereich IT-Sicherheit Vertiefung muss entweder das 10 KP Modul Case Study IT Security sowie ein weiteres Wahlpflichtmodul aus dem Bereich Security und Privacy bzw. Safety und Reliability oder das 16 KP Modul Case Study IT Security gewählt werden.

Modulnr.	**IT-Sicherheit Vertiefung**	**SWS**	**KP**	**Typ LZF**
CS4421-KP16	Case Study IT Security	2S +12P	16	A
CS4422-KP10	Case Study IT Security	2S +5P	10	A
	Wahlpflichtmodul aus dem Themenbereich Security und Privacy oder Safety und Reliability	variiert	6	A
	Zu erreichende Summe		**16**	

Neben den Modulen in den obigen Katalogen kann der Prüfungsausschuss weitere Module bestimmen, die für den Wahlpflichtbereich IT-Sicherheit gewählt werden können, soweit in diesen Veranstaltungen noch freie Kapazitäten vorhanden sind.

5. Pflicht-Lehrmodule aus dem Bereich Informatik

Aus den folgenden Wahlbereichen muss ein Modul gewählt werden. Bei den Basismodulen werden die jeweiligen Lehrveranstaltungen in der Regel semesterweise alternierend angeboten.

Modulnr.	**Basismodule Theoretische Informatik**	**SWS**	**KP**	**Typ LZF**
CS4000-KP06	Algorithmics	2V+2Ü	6	A
CS4020-KP06	Specification and Modelling	2V+2Ü	6	A
	Summe		**12**	

6. Wahlpflicht-Lehrmodule aus dem Bereich Informatik

Aus den folgenden zwei Wahlbereichen muss jeweils ein Modul gewählt werden. Bei den Basismodulen werden die jeweiligen Lehrveranstaltungen in der Regel semesterweise alternierend angeboten.

Modulnr.	**Basismodul Praktische Informatik**	**SWS**	**KP**	**Typ LZF**
CS4130-KP06	Information Systems	2V+2Ü	6	A
CS4150-KP06	Distributed Systems	2V+2Ü	6	A
	Zu erreichende Summe		**6**	

Modulnr.	**Basismodul Technische Informatik**	**SWS**	**KP**	**Typ LZF**
CS4160-KP06	Real-Time Systems	2V+2Ü	6	A
CS4170-KP06	Parallel Computer Systems	2V+2Ü	6	A
	Zu erreichende Summe		**6**	

7. Freier Vertiefungsbereich

Aus dem folgenden Vertiefungsbereich kann entweder ein 12 KP Modul oder zwei weitere Wahlpflichtmodule aus dem Bereich Security und Privacy bzw. Safety und Reliability belegt werden.

Modulnr.	**Vertiefung Informatik**	**SWS**	**KP**	**Typ LZF**
CS4501-KP12	Algorithmics, Logic and Computational Complexity	4V+2Ü+2S	12	A
CS4503-KP12	Ambient Computing	3V+2S+3P	12	A
CS4504-KP12	Cyber Physical Systems	4V+2Ü+2S	12	A
CS4505-KP12	System Architecture	4V+2Ü+2P	12	A
CS4508-KP12	Data Management	4V+2Ü+2S	12	A
CS4509-KP12	Internet Structures and Protocols / Internet Technologies	5V+1Ü+3P	12	A
CS4510-KP12	Signal Analysis	4V+2Ü+3P	12	A
CS4511-KP12	Learning Systems	4V+2Ü+2S	12	A
CS4514-KP12	Intelligent Agents	4V+2Ü+3P	12	A

	Vertiefung IT-Sicherheit			
	2 beliebige Wahlpflichtmodule aus dem Themenbereich Security und Privacy oder Safety und Reliability	variiert	6	A
	Zu erreichende Summe		**12**	

Neben den Modulen im obigen Katalog kann der Prüfungsausschuss weitere Module bestimmen, die für den Freien Vertiefungsbereich gewählt werden können, soweit in diesen Veranstaltungen noch freie Kapazitäten vorhanden sind.

8. Wahlbereich fächerübergreifend

Es müssen Module im Umfang von 4 Kreditpunkten gewählt werden, die fächerübergreifenden Charakter haben. Die Liste dieser Module ist auf den Webseiten des Studiengangs und des Hochschulrechts der Universität veröffentlicht.

9. Abschlussarbeit

ModulNr.	**Abschlussarbeit IT Security**	**KP**
CS5993-KP30	Master Thesis IT Security	**30**

Anhang 2 zur Studiengangsordnung für den
Masterstudiengang IT Security
der Universität zu Lübeck

Die folgende Tabelle beschreibt den empfohlenen Studienverlauf.