Studien- und Prüfungsordnung für den Masterstudiengang Cyber Security (Vollzeit / Teilzeit) an der Hochschule der Bayerischen Wirtschaft für angewandte Wissenschaften

(Studienbeginn ab Sommersemester 2020)

vom 27.04.2020

Aufgrund von Art. 80 Abs. 1 und 3, Art. 58 Abs. 1 Satz 1, Art. 61 Abs. 2 Satz 1 des Bayerischen Hochschulgesetzes (BayHSchG) vom 23. Mai 2006 (GVBl S. 245, BayRS 2210-1-1-K), zuletzt geändert durch § 1 Abs. 186 der Verordnung vom 26. März 2019 (GVBl. S. 98) und aufgrund des Einvernehmens des Bayerischen Staatsministeriums für Wissenschaft und Kunst vom 21.04.2020, erlässt die Hochschule der Bayerischen Wirtschaft für angewandte Wissenschaften (nachfolgend HDBW) folgende Studien- und Prüfungsordnung:

Inhalt

§ 1
Zweck der Studien- und Prüfungsordnung

Diese Studien- und Prüfungsordnung dient der Ausfüllung und Ergänzung der Rahmenprüfungsordnung für die Fachhochschulen (RaPO) vom 17. Oktober 2001 (GVBl S. 686, BayRS 2210-4-1-4-1-WK) und der Allgemeinen Prüfungsordnung der HDBW für den Masterstudiengang Cyber Security in der jeweils gültigen Fassung.

§ 2
Studienziel

(1) [1]Der Masterstudiengang Cyber Security vermittelt Kenntnisse und Fähigkeiten, die in dem Gebiet der Cyber Security erforderlich sind. Cyber Security wird für Unternehmen und Organisationen ein zusehends bedeutsameres und unerlässliches Gebiet, das sich gleichzeitig rasant weiterentwickelt und komplexer wird. [2]Der Masterstudiengang ist dem Profiltyp „anwendungsorientiert“ zugeordnet. Daher umfasst der Studiengang folgende Qualifikationsziele:

a. Die Studierenden kennen die unterschiedlichen System- und Netzwerkarchitekturen und können sie hinsichtlich ihrer Sicherheit und der Bedrohungspotentiale beurteilen.

b. Die Studierenden beherrschen die wesentlichen theoretischen Grundlagen aus dem Umfeld Verschlüsselung und deren praktischen Einsatz.

c. Die Studierenden kennen Methoden und Werkzeuge, mittels derer Angriffe auf die verschiedenen Systeme vorgenommen werden können.

d. Die Studierenden wenden Methoden und Werkzeuge zu Erkennung, Schutz und Abwehr von Angriffen auf verschiedenen Ebenen und Wegen an und kennen Vorgehensweisen zur Desaster Recovery.

e. Die Studierenden kennen die Bedeutung von Sicherheit im gesamten Lebenszyklus von Anwendungen und sind in der Lage, Cyber Security Anforderungen vom Entwurf bis End-of-Life umzusetzen.

f. Die Studierenden kennen die wesentlichen organisatorischen und rechtlichen Aspekte im nationalen und internationalen Kontext sowie die Anforderungen an Governance und Compliance, die im Umfeld Cyber Security relevant sind.Die Studierenden kennen neueste Ansätze z.B. aus der Künstlichen Intelligenz, und deren Anwendungsmöglichkeiten in der Cyber Security.

g. Die Studierenden haben ein anwendungsorientiertes Verständnis der aufgelisteten Aspekte und sind befähigt, diese als Mitarbeiter in verantwortender Position im Bereich Cyber Security technisch und organisatorisch selbständig umzusetzen.

(2) [1]Neben einer Vertiefung des Fachwissens werden im Masterstudium fachübergreifende wissenschaftliche und anwendungsorientierte Kenntnisse vermittelt, die die Qualifikation der Studierenden mit dem Ziel erweitern sollen, sie auch auf berufliche Spezialisierungen vorzubereiten. [2]Empirische Fragestellungen und Forschungsansätze kommen auf der Basis quantitativer Methoden sowie qualitativ-interpretativer Methoden in signifikanter Weise zum Einsatz und prägen den Masterstudiengang.

(3) [1]Der Masterstudiengang fördert zudem die für die berufliche Praxis wichtigen Fähigkeiten wie Sozialkompetenz, Kommunikationsfähigkeit und kooperative Teamarbeit. [2]Darüber hinaus soll der/die Studierende in die Lage versetzt werden, eigenständig für die Praxis nützliche, wissenschaftliche Methoden zu entwickeln. [3]Besonderer Nachdruck wird daher auf die Integration von Projektstudien gelegt.

§ 3
Qualifikation für das Studium

(1) Qualifikationsvoraussetzungen für den Zugang zum Masterstudiengang Cyber Security sind:

a. Der Nachweis eines mindestens 180 ECTS-Kreditpunkte und mindestens sechs theoretische Studiensemester umfassenden abgeschlossenen Studiums der Wirtschaftsinformatik, Informatik, Elektrotechnik und Informationstechnik oder Mechatronik mit Schwerpunkt IT an einer Hochschule oder eines gleichwertigen Abschlusses.

b. [1]Der Nachweis guter Englischkenntnisse in Wort und Schrift. [2]Der Nachweis wird durch die im europäischen Referenzrahmen festgelegten Sprachnachweise der Kompetenzstufe B2 erbracht (Anlage 2). [3]Der Nachweis gilt gleichfalls als erbracht, wenn ein erfolgreicher Abschluss einer englischsprachigen Ausbildung an einer höheren Schule oder Hochschule nachgewiesen wird oder die Muttersprache Englisch ist.

(2) [1]Über die Gleichwertigkeit von Hochschulabschlüssen und sonstigen Abschlüssen nach Abs. 1 a. und Nachweise nach b. entscheidet der Prüfungsausschuss (vgl. § 3 APO HDBW) unter Beachtung des Art. 63 Abs. 1 BayHSchG. [2]Von der Gleichwertigkeit von Hochschulabschlüssen (auch bei Erstabschlüssen ohne Ausweis der Leistungspunkte) ist auszugehen, sofern keine wesentlichen Unterschiede hinsichtlich der in diesem Studiengang erworbenen Kompetenzen festgestellt und begründet werden.

§ 4
Regelstudienzeit, Aufbau des Studiums, Akademischer Grad

(1) [1]Der Masterstudiengang wird in Vollzeit und Teilzeit angeboten. [2]Die Regelstudienzeit des Vollzeitstudiums beträgt drei theoretische Studiensemester einschließlich der Masterarbeit. [3]Die Regelstudienzeit des Teilzeitstudiums beträgt fünf theoretische Studiensemester einschließlich der Masterarbeit. [4]Einzelheiten regelt der Studienplan.

(2) [1]Soweit eine Studierende/ein Studierender ein abgeschlossenes Hochschulstudium nachweist, für das weniger als 210 ECTS-Kreditpunkte (jedoch mindestens 180 ECTS-

Kreditpunkte) vergeben wurden, ist Voraussetzung für das Bestehen der Masterprüfung der Nachweis der fehlenden ECTS-Kreditpunkte aus dem fachlich einschlägigen, grundständigen Studiengang Wirtschaftsinformatik/Business Intelligence der HDBW. [2]Der Prüfungsausschuss (vgl. §3 APO HDBW) stellt hierzu fest, welche Kompetenzen (Lernergebnisse) die/der Studierende in seinem abgeschlossenen Erststudium im Vergleich mit einem 210 ECTS-Kreditpunkte umfassenden Hochschulstudium nicht erworben hat und legt daraus die Module und Prüfungsleistungen fest, die von der/dem Studierenden nachzuholen und abzulegen sind. [3]Die von dem Prüfungsausschuss festgelegten Module und Prüfungsleistungen werden der/dem Studierenden mit der Immatrikulation bekannt gegeben. [4]Sie sind bis zum Eintritt in das dritte Studiensemester für Vollzeitstudierende und zum Eintritt in das fünfte Semester für Teilzeitstudierende nachzuholen.

(3) Ein Anspruch darauf, dass der Masterstudiengang bei einer nicht ausreichenden Zahl von Studienbewerberinnen und Studienbewerbern durchgeführt wird, besteht nicht.

(4) Bei erfolgreichem Abschluss der Masterprüfung wird der akademische Grad „Master of Science“, Kurzform „M.Sc.“ verliehen.

§ 5
Leistungspunkte

(1) [1]Für den erfolgreichen Abschluss von Modulen werden Leistungspunkte (ECTS-Punkte) vergeben. [2]Dabei entspricht ein Leistungspunkt einer Studienbelastung von etwa 30 Zeitstunden. [3]Die Anzahl der Leistungspunkte pro Modul ergibt sich aus Anlage 1 zu dieser Studien- und Prüfungsordnung.

(2) Für den erfolgreichen Abschluss des Studiengangs sind 90 Leistungspunkte nachzuweisen.

§ 6
Lehrveranstaltungen und Leistungsnachweise

(1) [1]Die Lehrveranstaltungen (Module), ihre Stundenzahl, die Art der Lehrveranstaltungen, die Anzahl der Leistungspunkte, die studienbegleitenden Leistungsnachweise sowie weitere Bestimmungen hierzu sind in der Anlage 1 zu dieser Studien- und Prüfungsordnung festgelegt. [2]Die Form der Prüfung wird am Anfang des Semesters durch den verantwortlichen Dozenten des Modules festgelegt und auf einem den Studenten zugänglichen Informationssystem der HDBW mitgeteilt. [3]Soweit Anlage 1 dieser Studien- und Prüfungsordnung keine abschließenden Bestimmungen enthält, trifft die weiteren Festlegungen das Modulhandbuch.

(2) Alle Module sind entweder Pflichtmodule oder Wahlpflichtmodule:

a. Pflichtmodule sind die Module des Studiengangs, die für alle Studierenden verbindlich sind.

b. [1]Wahlpflichtmodule sind die Module des Studiengangs, die einzeln oder in Gruppen alternativ angeboten werden. [2]Jeder Studierende muss unter ihnen nach Maßgabe dieser Studien- und Prüfungsordnung eine bestimmte Auswahl treffen. [3]Hat sich der/die Studierende bei Semesterbeginn für ein Modul entschieden, muss dieses belegt werden und geht in den Leistungsnachweis ein. [4]Es wird mindestens ein Wahlpflichtmodul durchgeführt. [5]Ein Anspruch darauf, dass alle Wahlpflichtmodule durchgeführt werden, besteht nicht.

(3) Alle Module und Prüfungen und/oder Leistungsnachweise können in englischer Sprache abgehalten werden; das Nähere regelt das Modulhandbuch. Die Prüfungen finden in den angegebenen Prüfungszeiträumen nach dem Ende der Vorlesungszeit oder semesterbegleitend statt.

§ 7
Masterthesis/Masterarbeit

(1) [1]Die Masterarbeit ist die wissenschaftliche Aufarbeitung des Studiums. [2]In ihr soll die bzw. der Studierende zeigen, dass sie/er in der Lage ist, eine anspruchsvolle Aufgabenstellung selbstständig zu bearbeiten und dazu Lösungsstrategien zu erarbeiten, zu beurteilen und effektiv umzusetzen.

(2) [1]Das Thema der Masterarbeit kann frühestens nach dem Ende der Vorlesungszeit des zweiten Semesters durch eine/n fachverantwortliche/n Professorin/Professor ausgegeben werden. [2]Voraussetzung für die Ausgabe des Themas ist der Erwerb von 60 ECTS-Kreditpunkten.

(3) [1]Die Masterarbeit wird von zwei hauptamtlichen Professorinnen/Professoren der HDBW bewertet, von denen die Erstprüferin/der Erstprüfer fachverantwortlich Lehr- und Prüfungsaufgaben in der gewählten Studienrichtung wahrnimmt. [2]Die Frist von der Themenausgabe bis zur Abgabe darf fünf Monate nicht überschreiten. [3]Auf schriftlichen Antrag der Kandidatin/des Kandidaten kann der Prüfungsausschuss die Bearbeitungszeit in begründeten Ausnahmefällen, wenn die Bearbeitungsfrist wegen Krankheit oder anderer vom Studierenden nicht zu vertretenden Gründen nicht eingehalten werden kann, im Einverständnis mit der Aufgabenstellerin/dem Aufgabensteller verlängern. [4]Die Nachfrist soll drei Monate nicht überschreiten. [5]Bei Nichteinhalten der Bearbeitungsfrist wird die Masterarbeit mit der Note „nicht ausreichend“ bewertet.

(4) [1]Die Bewertung einer Masterarbeit erfolgt durch ein schriftliches Gutachten, wobei die qualitativ und/oder quantitativ-empirische Forschungsmethodik besonders zu

betrachten ist. [2]Wird die Masterarbeit mit der Note „nicht ausreichend“ bewertet, so kann sie mit einem neuen Thema einmal wiederholt werden. [3]Die Vergabe des neuen Themas muss spätestens einen Monat nach Mitteilung des Ergebnisses der nicht bestandenen Masterarbeit erfolgen. [4]Hinsichtlich der Bearbeitungszeit gilt die Regelung des Absatzes 3.

§ 8
Abschlussmodul

Das Abschlussmodul besteht aus zwei Komponenten:

a. Der selbständigen Erstellung einer Masterarbeit im Umfang von bis zu 80 Seiten.

b. [1]Die Verteidigung und Präsentation der Ergebnisse der Masterarbeit mit einem Prüfungsgespräch, in dessen Rahmen die Inhalte der Masterarbeit auch in Verbindung zu sonstigen Inhalten des Studiums gesetzt werden. [2]Die Verteidigung wird von der Erstprüferin/dem Erstprüfer und einer weiteren hauptamtlichen Professorin/einem weiteren hauptamtlichen Professor abgenommen. [3]Die Präsentation der Ergebnisse der Masterarbeit soll 15 Minuten nicht überschreiten. [3]Die Gesamtdauer der Verteidigung darf 30 Minuten nicht überschreiten.

§ 9
Bestehen der Masterprüfung

Die Masterprüfung ist bestanden, wenn

a. in allen nach Anlage 1 Modulübersicht des Masterstudiengangs Cyber Security für das Bestehen der Masterprüfung erforderlichen Modulen einschließlich der Masterarbeit mindestens die Note „ausreichend" oder das Prädikat „bestanden“ erzielt wurde

b. und insgesamt 90 Leistungspunkte erworben wurden.

§ 10
Masterprüfungszeugnis

Über die bestandene Masterprüfung werden ein Zeugnis und ein Diploma Supplement ausgestellt.

§ 11
Inkrafttreten

Diese Studien- und Prüfungsordnung tritt rückwirkend zum 15.03.2020 in Kraft und gilt für Studierende des Masterstudiengangs Cyber Security an der HDBW mit Studienbeginn ab dem Sommersemester 2020.

Anlage 1:

Modulübersicht des Masterstudiengangs **Cyber Security (Vollzeit/Teilzeit)** an der ***Hochschule der Bayerischen Wirtschaft für angewandte Wissenschaften* – HDBW**

MoNr.	*Module mit Lehrveranstaltungen*	*LVF*	*V*	*SWS*	*MoP*	*LP**	*Sem VZ*	*Sem TZ*
CSM1	**Grundlagen Cyber Security - Introduction to Cyber Security**				**sP**	**5**	**1**	**1**
CSM1	Grundlagen Cyber Security - Introduction to Cyber Security	VL/UE	P	4				
CSM2	**Kryptographie - Cryptography**				**sP**	**5**	**1**	**1**
CSM2	Kryptographie - Cryptography	VL/UE	P	4				
CSM3	**Computersysteme und Netzwerke - Systems and Networks**				**sP**	**5**	**1**	**1**
CSM3	Computersysteme und Netzwerke - Systems and Networks	VL/UE	P	4				
CSM4	**Systemanalyse und Härtung - System Auditing and Hardening**				**PA**	**5**	**1**	**1**
CSM4	Systemanalyse und Härtung - System Auditing and Hardening	VL/UE	P	4				
CSM5	**Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle**				**sP**	**5**	**1**	**3**
CSM5	Anwendungsentwicklung und Sicherheitslebenszyklus - Application Development & Security Lifecycle	VL/UE	P	4				
CSM6	**Wahlpflichtmodul**					**5**	**1**	**3**
CSM6-1	Python und Go – Python and Go	VL/UE	WP	2	**PA**	**2,5**	**1**	**3**
CSM6-2	Human Factors in Cyber Security	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-3	Ethik – Ethics	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**
CSM6-4	Softskills – Softskills	VL/UE	WP	2	**PR**	**2,5**	**1**	**3**

CSM7	**Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,…) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)**				**PA**	**5**	**2**	**4**
CSM7	Sicherheitsaspekte in Anwendungsfeldern (Industrial Internet,IoT, mobile und Cloud,…) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	PA	P	4				
CSM8	**Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy**				**sP**	**5**	**2**	**2**
CSM8	Rechtliche Aspekte & Datenschutz - Legal Aspects & Privacy	VL/UE	P	4				
CSM9	**Seminar: aktuelle Themen der Cyber Security**				**PA**	**5**	**2**	**4**
CSM9	Seminar: aktuelle Themen der Cyber Security	VL/UE	P	4				
Wahlpflichtbereich Technik								
CSMT1	**Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics**				**PA**	**5**	**2**	**2**
CSMT1	Intrusion Detection + Digitale Forensik - Intrusion Detection + Digital Forensics	VL/UE	P	2				
CSMT2	**System- und Netzwerksicherheit - System and Network Security**				**PA**	**5**	**2**	**2**
CSMT2	System- und Netzwerksicherheit - System and Network Security	VL/UE	P	4				
CSMT3	**Methoden der Künstlichen Intelligenz (KI)**				**sP**	**5**	**2**	**2**
CSMT3	Methoden der Künstlichen Intelligenz (KI)	VL/UE	P	4				
Wahlpflichtbereich Organisation und Management								
CSMO1	**Reifegradmodelle - Security Maturity**				**sP**	**5**	**2**	**2**
CSMO1	Reifegradmodelle - Security Maturity	VL/UE	P	2				

CSMO2	**Security Governance and Compliance**				**sP**	**5**	**2**	**2**
CSMO2	Security Governance and Compliance	VL/UE	P	4				
CSMO3	**Sicherheitsmanagement - Security Manangement**				**sP**	**5**	**2**	**2**
CSMO3	Sicherheitsmanagement - Security Manangement	VL/UE	WP	4				
CSM10	**Incident Management and Desaster Recovery**				**PA**	**5**	**3**	**3**
CSM10	Incident Management and Desaster Recovery	VL/UE	WP	4				
CSM11	**Requirements Engineering and Threat Modelling**				**sP**	**5**	**3**	**3**
CSM11	Requirements Engineering and Threat Modelling	VL/UE	WP	4				
CSMMT	**Master-Thesis**						**3**	**5**
CSMMT1	Masterthesis	SSt	P		**HA**	**18**		
CSMMT2	Verteidigung / defense	mP	P		**mP**	**2**		

** Leistungspunkte (LP) werden nach dem European Credit Transfer System (ECTS) vergeben.*

Legende

A	Anwendungsorientierte Spezialisierung	AM	Abschlussmodul
B	Betriebswirtschaft	BP	Betriebspraktikum
BS	Blockseminar	MT	Masterthesis
BL	Blended Learning	F	Fachliche Spezialisierung
G	Grundlagenstudium	HA	Hausarbeit
KO	Kolloquium	L	Laborunterricht
LP	Leistungspunkte	LVF	Lehrveranstaltungsform
MoNr.	Modul Nummer	mP	Mündliche Prüfung
MoP	Modulprüfung	N.N.	Nicht benannt
P	Pflichtveranstaltung	PA	Projektarbeit
PB	Praktikumsbericht	PL	Praxisorientierte Lehrveranstaltung
PR	Präsentation	PS	Praxissemester
R	Referat oder Kurzreferat	S	Seminar

SK	Sprachkurs	sP	Schriftliche Prüfung
SPJ	Studienprojekt	SSt	Selbststudium
SWS	Semesterwochenstunden	TZ	Teilzeit
UE	Übung	V	Verbindlichkeit
VE	Verteidigung	VL	Vorlesung
VZ	Vollzeit	WL	Workload
WP	Wahlpflichtveranstaltung		

Anlage 2:

Übersicht über die Anerkennung von englischen Sprachnachweisen, die im europäischen Referenzrahmen entsprechend der Kompetenzstufe B2 erbracht werden müssen:

[1]Die Studien-und Prüfungsordnung sieht als Sprachnachweise der Kompetenzstufe B2 folgende standardisierte Testverfahren mit den entsprechenden „Mindest-Scores“ vor:

- Test of English as a Foreign Language (TOEFL) internet based mind. 89 Punkte oder
- International English Language Testing System (IELTS) mind. 7.0 oder
- Test of English for International Communications (TOEIC), Mindestscore: 700 Punkte

[2]Der Nachweis der geforderten Sprachkompetenz kann auch durch ein Cambridge First Certificate in English (FCE), durch ein Cambridge Certificate of Proficiency (CPE) oder das Business English Certificate (BEC) Vantage erfolgen.