Study and examination regulations for the Master's degree program in Cyber Security (full-time / part-time) at the HDBW University of Applied Sciences

valid for students starting their studies from winter semester 24/25

from 16.09.2024

This translation serves to inform our international students. The valid legal reference can be found in the original „Studien- und Prüfungsordnung für den Masterstudiengang Digital Business Modelling and Entrepreneurship (Vollzeit / Teilzeit) an der Hochschule der Bayerischen Wirtschaft für angewandte Wissenschaften“

Based on Art. 9, Art. 80 para. 1, Art. 84 para. 2, para. 3, para. 4, para. 6, Art. 85, Art. 86 of the Bavarian Higher Education Innovation Act (BayHIG) of August 5, 2022 (GVBl. p. 414, BayRS 2210-1-3-WK) and based on the agreement of the Bavarian State Ministry of Science and the Arts of July 29, 2024, the HDBW University of Applied Sciences (hereinafter HDBW) issues the following study and examination regulations:

Contents

§ 1
Purpose of the study and examination regulations

These study and examination regulations serve to complete and supplement the General Examination Regulations of the HDBW (APO) for the Master's degree program in Cyber Security in the currently valid version.

§ 2
Study objective

(1) [1]The Master's degree program in Cyber Security imparts the knowledge and skills required in the field of cyber security. [2]Cyber security is becoming an increasingly important and indispensable field for companies and organizations, while at the same time developing rapidly and becoming more complex. [3]The Master's degree program is assigned to the "application-oriented" profile type. [4]The degree program therefore includes the following qualification objectives:

a. Students are familiar with the various system and network architectures and can assess them in terms of their security and potential threats.

b. Students master the essential theoretical principles of encryption and their practical application.

c. Students know methods and tools that can be used to attack the various systems.

d. Students use methods and tools to detect, protect and defend against attacks at various levels and in various ways and are familiar with disaster recovery procedures.

e. Students know the importance of security throughout the entire life cycle of applications and are able to implement cyber security requirements from design to end-of-life.

f. Students know the key organizational and legal aspects in a national and international context as well as the governance and compliance requirements that are relevant in the cyber security environment.

g. Students are familiar with the latest approaches, e.g. from artificial intelligence, and their possible applications in cyber security.

h. Students have an application-oriented understanding of the aspects listed and are able to implement them independently as employees in a responsible position in the field of cyber security, both technically and organizationally.

(2) [1]In addition to a deepening of specialist knowledge, the Master's programme teaches interdisciplinary scientific and application-oriented knowledge, which is intended to expand students' qualifications with the aim of preparing them for professional specializations. [2]Empirical questions and research approaches based on quantitative methods as well as qualitative-interpretative methods are used in a significant way and characterize the Master's degree course.

(3) [1]The Master's degree program also promotes skills that are important for professional practice, such as social competence, communication skills and cooperative teamwork. [2]In addition, students should be able to independently develop scientific methods that are useful in practice. [3]Particular emphasis is therefore placed on the integration of project studies.

§ 3
Qualification for the study program

(1) Qualification requirements for admission to the Master's degree program in Cyber Security are:

a. Proof of having completed a degree in business informatics, computer science, electrical engineering and information technology or mechatronics with a focus on IT at a university or an equivalent degree comprising at least 180 ECTS credits and at least six theoretical semesters of study.

b. [1]Proof of good written and spoken English language skills. [2]Proof is provided by the language certificates of competence level B2 specified in the European Framework of Reference (Annex 2). [3]Proof is also deemed to have been provided if the applicant has successfully completed an English-language course at a secondary school or university or is a native English speaker.

(2) [1]The Examination Board (see § 3 APO) decides on the equivalence of university degrees and other degrees according to para. 1 a. and proof according to b. in compliance with Art. 86 para. 1 BayHIG. [2]The equivalence of university degrees (including first degrees without credit points) shall be assumed provided that no significant differences are identified and justified with regard to the competencies acquired in this degree program.

§ 4
Standard period of study, structure of the degree program, academic degree

(1) [1]The Master's degree program is offered full-time and part-time. [2]The standard period of study for the full-time course is three theoretical semesters including the Master's thesis. [3]The standard period of study for the part-time course is five theoretical semesters including the Master's thesis. [4]Details are set out in the curriculum.

(2) [1]If a student can provide evidence of a completed university degree for which fewer than 210 ECTS credits (but at least 180 ECTS credits) have been awarded, the prerequisite for passing the Master's examination is proof of the missing ECTS credits from the relevant undergraduate degree course in Business Informatics/Business Intelligence at the HDBW. [2]The Examination Board (see § 3 APO) determines which competencies (learning outcomes) the student has not acquired in his/her completed first degree compared to a university degree program comprising 210 ECTS credits and determines the modules and examinations to be completed by the student. [3]The modules and examinations determined by the examination board will be communicated to the student upon enrolment. [4]They must be completed by the start of the third semester for full-time students and by the start of the fifth semester for part-time students.

(3) There is no entitlement for the Master's degree program to be carried out if the number of applicants is insufficient.

(4) Upon successful completion of the Master's examination, the academic degree "Master of Science", abbreviated to "M.Sc.

§ 5
Credit points

(1) [1]Credit points (ECTS points) are awarded for the successful completion of modules. [2]One credit point corresponds to a study load of approximately 30 hours. [3]The number of credit points per module can be found in Appendix 1 to these study and examination regulations.

(2) Successful completion of the degree program requires 90 credit points.

§ 6
Courses and certificates of achievement

(1) The courses (modules), their number of hours, the type of courses, the number of credit points, the course-related certificates of achievement and further provisions are set out in Annex 1 to these study and examination regulations.

(2) All modules are either compulsory modules or compulsory elective modules:

a. Compulsory modules are the modules of the degree program that are mandatory for all students.

b. [1]Compulsory elective modules are the modules of the degree program that are offered individually or in groups as an alternative. [2]Each student must make a specific selection from among them in accordance with these study and

examination regulations. [3]Once the student has decided on a module at the beginning of the semester, this module must be taken and is included in the transcript of records. [4]At least one compulsory elective module must be completed. [5]There is no entitlement to take all compulsory elective modules.

(3) [1]All modules, examinations and/or performance assessments are held in English; further details can be found in the module handbook. [2]The examinations take place in the specified examination periods after the end of the lecture period or during the semester.

(4) [1]The form of the examination is announced by the examination board in accordance with Section 5 (3) APO. [2]A combination of different examinations is possible (partial examinations).

(5) [1]Insofar as Annex 1 of these study and examination regulations does not contain any conclusive provisions, the module handbook shall contain further specifications. [2]If several partial examinations are required to pass the module, it must be clearly defined how the parts are weighted and whether it is necessary to pass all parts in order to pass the module as a whole.

§ 7
Final module

(1) The final module consists of two components in accordance with § 24 APO:

a. [1]The independent preparation of a Master's thesis. This comprises at least 70 pages of content and should not exceed 120 pages. [2]Cover sheet, all lists, index and additional pages in the introduction and credits do not count.

b. [1]The defense and presentation of the results of the Master's thesis with an examination discussion in which the content of the Master's thesis is also linked to other content of the degree program. [2]The defense and presentation of the results of the Master's thesis should not exceed 15 minutes. [3]The total duration of the defense should not exceed 30 minutes

(2) [1]The topic of the Master's thesis can be issued by a professor responsible for the subject at the earliest after the end of the lecture period of the second semester. [2]A prerequisite for the issue of the topic is the acquisition of 50 ECTS credits.

(3) [1]The Master's thesis is assessed in a written report, in which the qualitative and/or quantitative-empirical research methodology is to be presented in particular. [2]If the Master's thesis is assessed as "insufficient", it can be repeated once with a new topic. [3]The new topic must be assigned no later than one month after notification of the result of the failed Master's thesis. [4]With regard to the processing time, the regulations for the first attempt apply.

§ 8
Passing the Master's examination

The Master's examination is passed if

a. at least the grade "sufficient" or the grade "passed" was achieved in all modules required for passing the Master's examination according to Annex 1 Module Overview of the Master's degree program in Cyber Security, including the Master's thesis

b. and a total of at least 90 credit points have been earned.

§ 9
Entry into force

These study and examination regulations come into force on 16.09.2024 and apply to students of the Master's degree program Cyber Security at the HDBW starting in the winter semester 24/25.

Appendix 1:

Module overview of the Master's degree program **Cyber Security (full-time/part-time)** at the ***Bavarian University of Applied Sciences* - HDBW**

MoNo.	*Modules with courses*	*LVF*	*V*	*SWS*	*MoP*	*LP**	*Sem VZ*	*Sem TZ*
CSM1	**Basics of Cyber Security - Introduction to Cyber Security**				**sP 90 min. or (PR 20 min and mP 10 min)**	**5**	**1**	**1**
CSM1	Basics of Cyber Security - Introduction to Cyber Security	VL/UE	P	4				
CSM2	**Cryptography - Cryptography**				**sP 90 min or mP 30 min**	**5**	**1**	**3**
CSM2	Cryptography - Cryptography	VL/UE	P	4				
CSM3	**Computer Systems and Networks - Systems and Networks**				**sP 90 min or (PA 10-15 p. and PR 20 min)**	**5**	**1**	**1**
CSM3	Computer Systems and Networks - Systems and Networks	VL/UE	P	4				
CSM4	**System Analysis and Hardening - System Auditing and Hardening**				**sP 90 min or mP 30 min**	**5**	**1**	**1**
CSM4	System Analysis and Hardening - System Auditing and Hardening	VL/UE	P	4				
CSM5	**Application Development and Security Lifecycle - Application Development & Security Lifecycle**				**sP 90 min or mP 30 min**	**5**	**1**	**3**
CSM5	Application Development and Security Lifecycle - Application Development & Security Lifecycle	VL/UE	P	4				
CSM6	**Compulsory elective module**					**5**	**1**	**3**
CSM6-1	Cloud hacking	VL/UE	WP	2	**mP 20 min or HA 10-15 p.**	**2,5**	**1**	**3**
CSM6-2	Human Factors in Cyber Security	VL/UE	WP	2	**mP 20 min or HA 10-15 p.**	**2,5**	**1**	**3**
CSM6-3	Technology Ethics - Technology Ethics	VL/UE	WP	2	**mP 20 min or HA 10-15 p.**	**2,5**	**1**	**3**
CSM6-4	Softskills - Softskills	VL/UE	WP	2	**mP 20 min or HA 10-15 p.**	**2,5**	**1**	**3**
CSM6-5	Linux Basics - Linux Basics	VL/UE	WP	2	**mP 20 min.**	**2,5**	**1**	**3**
CSM6-6	Web Technologies - Web Technologies	VL/UE	WP	2	**mP 20 min.**	**2,5**	**1**	**3**
CSM6-7	Introduction to Docker - Introduction to Docker	VL/UE	WP	2	**mP 20 min.**	**2,5**	**1**	**3**
CSM6-8	Cyber Threat Intelligence	VL/UE	WP	2	**mP 20 min or HA 10-15 p.**	**2,5**	**1**	**3**
CSM8	**Legal aspects & data protection - Legal Aspects & Privacy**				**sP 90 min o. (HA 20-30 p. and PR 10 min)**	**5**	**2**	**2**
CSM8	Legal aspects & data protection - Legal Aspects & Privacy	VL/UE	P	4				
CSM9	**Seminar: current topics in cyber security**				**sP 90 min o. (HA 20-30 p. and PR 10 min)**	**5**	**2**	**2**
CSM9	Seminar: current topics in cyber security	VL/UE	P	4				
CSM11	**Requirements Engineering and Threat Modeling**					**5**	**2**	**3**

CSM11	Requirements Engineering and Threat Modeling	VL/UE	WP	4	**sP 90 min o. (HA 20-30 p. and PR 10 min)**			
CSM10	**Incident Management and Disaster Recovery**				**sP 90 min o. HA 20-30 p.**	**5**	**3**	**3**
CSM10	Incident Management and Disaster Recovery	VL/UE	WP	4				
CSM7	**Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)**				**sP 90 min or (PA 10-15 p. and PR 20 min)**	**5**	**3**	**3**
CSM7	Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...) - Security Aspects in Application Areas (Industrial Internet, IoT, Mobile and Cloud,...)	VL/UE	P	4				
CSMMT	**Master thesis**						**3**	**5**
CSMMT1	Master's thesis	SSt	P		**70-120 S.**	**18**		
CSMMT2	Verteidigung / defense	mP	P		**mP 20-30 min**	**2**		
Technology elective area								
CSMT1	**Intrusion Detection + Digital Forensics - Intrusion Detection + Digital Forensics**				**sP 90 min or (PA 10-15 p. and PR 20 min)**	**5**	**2**	**4**
CSMT1	Intrusion Detection + Digital Forensics - Intrusion Detection + Digital Forensics	VL/UE	P	4				
CSMT2	**System and Network Security - System and Network Security**				**sP 90 min or mP 30 min**	**5**	**2**	**2**
CSMT2	System and Network Security - System and Network Security	VL/UE	P	4				
CSMT3	**Methods of artificial intelligence (AI)**				**sP 90 min or (PA 10-15 p. and PR 20 min)**	**5**	**2**	**2**
CSMT3	Methods of artificial intelligence (AI)	VL/UE	P	4				
Compulsory elective area Organization and Management								
CSMO1	**Maturity models - Security Maturity**				**sP 90 min o. (HA 20-30 p. and PR 10 min)**	**5**	**2**	**2**
CSMO1	Maturity models - Security Maturity	VL/UE	P	4				
CSMO2	**Security Governance and Compliance**				**sP 90 min o. (HA 20-30 p. and PR 10 min)**	**5**	**2**	**2**
CSMO2	Security Governance and Compliance	VL/UE	P	4				
CSMO3	**Security Management - Security Manangement**				**sP 90 min o. (HA 20-30 p. and PR 10 min)**	**5**	**2**	**2**
CSMO3	Security Management - Security Manangement	VL/UE	WP	4				

** Credit points (CP) are awarded according to the European Credit Transfer System (ECTS).*

Legend

A	Application-oriented specialization	AM	Final module
B	Business administration	BP	Work placement
BS	Block seminar	MT	Master's thesis
BL	Blended learning	F	Professional specialization
G	Basic studies	HA	Term paper
KO	Colloquium	L	Laboratory lessons
LP	Credit points	LVF	Type of course
MoNo.	Module number	mP	Oral examination
MoP	Module examination	N.N.	Not named
P	Compulsory event	PA	Project work
PB	Internship report	PL	Practice-oriented course
PR	Presentation	PS	Practical semester
R	Presentation or short paper	S	Seminar
SK	Language course	sP	Written examination
SPJ	Study project	SSt	Self-study
SWS	Semester hours per week	TZ	Part-time
UE	Exercise	V	Liability
VE	Defense	VL	Lecture
VZ	Full-time	WL	Workload
WP	Compulsory elective course		

Appendix 2:

Overview of the recognition of English language certificates that must be provided in accordance with the European Framework of Reference for Languages at level B2:

[1]The study and examination regulations stipulate the following standardized test procedures with the corresponding "minimum scores" as proof of language competence level B2:

- Test of English as a Foreign Language (TOEFL) internet based at least 89 points or
- International English Language Testing System (IELTS) at least 7.0 or
- Test of English for International Communications (TOEIC), minimum score: 700 points

[2]Proof of the required language competence can also be provided by a Cambridge First Certificate in English (FCE), a Cambridge Certificate of Proficiency (CPE) or the Business English Certificate (BEC) Vantage.

Issued on the basis of the decision of the HDBW Senate on 13.12.2023 and on the basis of the agreement of the Bavarian State Ministry of Science and the Arts of 29.07.2024, AZ L.3-H6484.3.15/2/12.

Munich, 16.09.2024 ……..……..……..……..……..…..

Prof. Dr. Kerstin Fink, President

The statutes were deposited at the university on 16.09.2024. The resignation was announced on 16.09.2024 by means of a notice at the university. The date of the announcement is accordingly 16.09.2024.