# Subject-Related Examination and Study Regulations for the Master's Degree Programme Cyber Security of 22 September 2017

## English translation, not legally binding!

In accordance with the Brandenburg Higher Education Act (Brandenburgisches Hochschulgesetz – BbgHG) of 28 April 2014 (GVBl. I/14 Nr. 18), last amended by the act of 1 July 2015 (GVBl. I/15 Nr. 18), according to Section 5 Paragraph 1 Sentence 2, Section 9 Paragraph 5 Sentence 2 in conjunction with Section 19 Paragraph 2 Sentence 1, Section 22 Paragraph 2 Sentence 1, Section 72 Paragraph 2 Sentence 1 and Section 1 of the General Examination and Study Regulations for Master's Degree Programmes at the Brandenburg University of Technology Cottbus-Senftenberg from 12. September 2016 (AMbl. 14/2016), Brandenburg University of Technology Cottbus-Senftenberg (BTU) has adopted the following statutes:

### Contents



### § 1 Scope of Validity

[1]These statutes outlines the subject-related specifics for the Cyber Security Master's Programme. [2]It is a supplement to the General Examination and Study Regulations for Master's Degree Programmes at BTU (RahmenO-MA) from 12 September 2016 (AMBl. 14/2016). [3]In case of conflicts between the two regulations, the general study regulations have priority.

## § 2 Content Profile of the Programme, Goals of Studies

[1]The aim of the Cyber Security study programme is to facilitate the learning and strengthening of relevant knowledge, skills and methods related to IT security. In addition, the programme aims to foster students' ability to work independently in the IT security sector and to incorporate them into current research. [2]Graduates of this programme are qualified to assess IT system vulnerabilities and to find and assess solutions for bringing these systems up to the standards required by the relevant organisational and legal standards, using modern technology. [3]The study programme couples computer science and engineering both in theory and practice. [4]It is designed to make graduates capable of taking on important and difficult problems in industrial, administrative, and research settings, by implementing existing or their own innovative IT security strategies.

## § 3 Graduation, Degree

Upon successful completion of the study programme the academic degree "Master of Science" (M. Sc.) will be awarded.

## § 4 Further Admission and Enrolment Requirements

(1) Only students who are enrolled according to the BTU framework regulations are allowed to participate in the programme.

(2) [1]Principal requirement for admission to this Master's programme is a degree that proves qualification for work in a computer science related field (at least Bachelor's degree). [2]Applicants with a degree in Computer Science, IT security, or Mathematics with a minor in Computer Science are especially qualified. [3]Sufficient qualifications are met if the student's previous degree is verifiably similar in content to the Computer Science Bachelor's programme offered at the BTU in terms of theory and practical exercises for computer science and mathematics.

(3) [1]The verification of adequate qualifications is carried out by the Examination Board. [2]In the case the qualifications do not completely satisfy the prerequisites, the Examination Board can require that certain additional modules be taken.

(4) [1]Cyber Security is an international study programme. [2]The language of teaching and examination is English. [3]For admission into the study programme it is required that students provide proof of sufficient English language skills according to Section 3 Paragraph 3 of the Enrolment Regulations at the BTU of 13 July 2015 (AMBl. 01/2015).

## § 5 Regular Duration and Scope of the Programme

(1) [1]The regular duration of studies for this programme is 4 semesters. [2]The scope of the Master's programme is 120 credit points, in accordance with ECTS (European Credit Transfer System).

(2) [1]The programme begins in the Winter Semester. [2]It is a full-time study programme.

## § 6 Programme Structure and Organisation

(1) [1]The design of the Master's programme is 4 semesters with 30 credit points in each. [2]The structure of the programme is described in the syllabus (Annex 1). [3]The syllabus is designed to have both a focus on fundamentals and specialisations as well as practical training, such as general modules, an internship in the industry and the Master Thesis.

(2) The module area for fundamentals "Cyber Security Basics" consits of the mandatory modules listed in Annex 2, with a scope of 22 credit points.

(3) [1]The specialisation part of the programme has a scope of 54 credit points and is divided into two areas with compulsory elective modules (see Annex 2) and the Study Project. [2]From the module area "Cyber Security Methods", at least 28 credit points and from the module area "Computer Science", at least 12 credit points are required.

(4) The internship is at least two months long, and should be completed in the free time between lecture periods.

## § 7 Special Regulations for the Organisation of Examinations

There are no special regulations for the organisation of examinations.

## § 8 Master Thesis

(1) [1]The Master Thesis must be written in English and is generally to be completed in the 4th semester. [2]It has a scope of 30 credit points. [3]The working time for the written portion of the thesis is 5 months. [4]The registration of the thesis can only be done when all modules including the Study Project have been successfully completed by earning 82 credit points. [5]The internship in the industry can be completed after the completion of the Master Thesis.

(2) [1]The topic of the Master Thesis must be related to the field of Cyber Security (IT security). [2]This must be verified by the Examination Board upon registration of the thesis.

## § 9 Further Supplementary Regulations

There are no additional regulations.

## § 10 Entry into Force, Abrogation, Transitional Regulations

(1) These regulations come into effect the day after they are published.

(2) These Examination and Study Regulations are no longer relevant 4 semesters after the established regular study duration of the programme and the final enrolment.

Issued on the basis of the decisions made by the Faculty Council of Faculty 1 – Mathematics, Computer Science, Physics, Electrical Engineering and Information Technology held on 12 October 2016 and 12 July 2017, the opinion provided by the Senate on 15 December 2016 and the approval of the President of Brandenburg University of Technology Cottbus-Senftenberg

given on 7 March 2017, and the approval of the Ministry of Science, Research and Culture of the federal state of Brandenburg given on 30 May 2017.

## Annex 1: Overview of the Modules, Status, Credit Points (CP)

| Module Areas/Modules | Status | Evaluation | Credit Points |
|---|---|---|---|
| **Basic Modules** | | | **22** |
| Cyber Security Basics | P | Examination | 22 |
| **Specialisation Modules** | | | **54** |
| Cyber Security Methods | WP | Examination* | 28–34 |
| Computer Science | WP | Examination* | 12–18 |
| Study Project | P | Study Performance | 8 |
| | | | **44** |
| General Studies | WP | Examination | 6 |
| Internship | P | Study Performance | 8 |
| Master Thesis | P | Examination | 30 |
| Sum | | | **120** |

P = Mandatory, WP = Compulsory Elective
*) Seminars and Laboratory Courses that are assessed with a Study Performance can be considered to the extent of a maximum of 12 credit points as Specialisation Modules.

## Annex 2: Modules for Basic and Specialisation Studies

| Module Title | Credit Points |
|---|---|
| **Cyber Security Basics (Mandatory)** | |
| Introduction into Cyber Security | 8 |
| Cryptography | 8 |
| IT Security Law | 6 |
| **Cyber Security Methods (Compulsory Elective)** | |
| Cryptographic Protocols | 6 |
| Pervasive System Security | 6 |
| Security of Resource-constraint Systems | 6 |
| Software Security | 6 |
| Hands on Knowledge for Side Channel Attacks | 6 |
| Cyber Security Application Areas | 6 |
| Cyber Security Lab | 6 |
| Seminar | 4 |
| **Computer Science (Compulsory Elective)** | |
| Introduction to Web Services and eBusiness Technologies | 6 |
| Web-Technologies Lab | 4 |
| Dependability and Fault Tolerance | 6 |
| Foundations of Data Mining | 6 |
| Neural Networks and Learning Theory | 8 |
| Software Project Management | 8 |
| Internet - Functionality, Protocols, Applications | 8 |
| Wireless Sensor Networks: Concepts, Protocols and Applications | 6 |
| Introduction into Concurrency | 8 |
| Software Dependability | 8 |
| Software Testing | 8 |
| Operating Systems II (Multi-Level Memory Management) | 6 |
| Distributed and Parallel Systems II (Concurrency, Replication and Consistency) | 6 |

The head of the study programme may extent the list of Compulsory Elective Modules upon request.

## Annex 3: Regular Study Plan

| **Modules** | **CP per Semester** | | | | **CP Sum** |
|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | |
| **Basic Modules: Cyber Security Basics** (Mandatory) | | | | | |
| Introduction into Cyber Security | 8 | | | | 8 |
| Cryptography | | 8 | | | 8 |
| IT Security Law | | | 6 | | 6 |
| **Sum Basic Modules** | 8 | 8 | 6 | | 22 |
| | | | | | |
| **Specialisation Modules** | | | | | |
| Compulsory Elective Modules Cyber Security Methods | 16 | 10 | 8 | | 34 |
| Compulsory Elective Modules Computer Science | 6 | 6 | | | 12 |
| Study Project | | | 8 | | 8 |
| **Sum Specialisation Modules** | **22** | **16** | **16** | | **54** |
| | | | | | |
| General Studies | | 6 | | | 6 |
| Internship | | | 8 | | 8 |
| Master Thesis | | | | 30 | 30 |
| **Sum** | | **6** | **8** | **30** | **44** |
| **Total Sum of Studies** | **30** | **30** | **30** | **30** | **120** |

## Annex 4: Internship Regulations for the Professional Internship

### 1. Validity

These regulations apply to the professional internship of the Master's programme Cyber Security at the Brandenburg University of Technology Cottbus-Senftenberg in conjunction with the current Examination and Study Regulations.

### 2. Purpose of the Internship

The professional internship is intended to give students the opportunity to use and implement the knowledge gained in the classroom. In particular, it strengthens the ability to work as a team. The internship serves as an opportunity to get an understanding for the connection between the industry side, and the research and academia side of IT security. It is the students' responsibility to find an appropriate internship place. The chairs of the programme can and should help facilitate this connection.

### 3. Registration

The internship must be approved by a mentor at least 4 weeks before its start. The approval entails the screening of the type of work, the company, and the supervisor at the company.

### 4. Internships Abroad

In general, internships abroad are welcomed. However, they must follow the same prerequisites as those in Germany. Exchange programmes and agencies can be found through the Deutscher Akademischer Austauschdienst (DAAD).

### 5. Internship Places

Potentially suitable companies for an internship are those that operate in the field of IT security, but also non-university research institutions (e.g. institutes of the Fraunhofer-Gesellschaft). Only in exceptional cases students are permitted to intern at higher education institutions (e.g. IT services in universities). The interning student should receive mentoring from supervisor that is employed by the company or institution, and has earned a Diploma or Master's degree in a relevant field. This supervisor must be mentioned in the report and be available as a contact person. He or she should guide the students in their thesis and be readily available to answer questions and make recommendations.

### 6. Supervision

The supervision on the BTU's side is the responsibility of the mentor. Research assistants are permitted to assist in the supervision. It is expected that the mentor at the BTU and the supervisor at the respective institution or company regularly engage in consultations with each other.

### 7. The Duration and Division of the Intership

The internship must have a duration of at least 2 months. If possible, it should be completed without interruptions. A week of interning is equivalent to a regular workweek at the company

providing the internship. The vacation time is determined in accordance with the German Federal Holiday Act (Bundesurlaubsgesetz) Longer periods of missed work due to illness must be made up for, shorter periods are ruled upon by the Examination Board. It is advised to do scheduling during the internship and keep a journal.

**8. Internship Report**

For the whole duration of the internship it is required that the student writes a report (about 3,500–4,000 words) to be submitted to the supervisor at the company. The report must satisfy the general requirements for scientific work. With permission from the supervisor at the company providing the internship, it is possible to write the report in English. It should describe:

– the company where the internship takes place,

– the sector that company operates in and if relevant the department within the company,

– the task, the existing state of the technology,

– the approach, solution,

– reflection on one owns work, experiences, knowledge gained, applicability of knowledge/skills gained from the study programme.

The supervisor at the company providing the internship must sign off on the report before it is submitted. The report must be submitted to the mentor at the BTU at the latest 8 weeks after the completion of the internship.