Study Regulations Governing the Bachelor's Degree 'Cybersecurity (English)'

25 February 2021

Note: This translation is provided for information purposes only. In the event of any discrepancy between the translation and the original German version published in the Official Bulletin (*Dienstblatt der Hochschulen des Saarlandes*), the provisions of the latter shall take precedence.

Pursuant to Section 60 of the Saarland Higher Education Institutions Act (SHSG) of 30 November 2016 (Official Gazette of Saarland I, p. 1080) most recently amended in law on 8–9 December 2020 (Official Gazette I (2021), p. 53) and on the basis of the Joint Examination Regulations for Bachelor's and Master's Degree Programmes of the Faculty of Mathematics and Computer Science of 25 February 2021 (Official Bulletin No. 62, p. 580) and with the consent of the Saarland University Senate, the Faculty of Mathematics and Computer Science at Saarland University hereby issues the following Study Regulations for the Bachelor's Degree Programme 'Cybersecurity (English)'.

Section 1
Scope

These study regulations, which govern the content and structure of the Bachelor's degree programme 'Cybersecurity (English)', are based on the Joint Examination Regulations for the Bachelor's and Master's Degree Programmes of the Faculty of Mathematics and Computer Science of 25 February 2021 (Official Bulletin No. 62, p. 580) and the Subject-Specific Regulations Governing the Bachelor's Degree Programme 'Cybersecurity (English)' of 25 February 2021 (Official Bulletin No. 66, p. 626). The Faculty of Mathematics and Computer Science is responsible for organizing the teaching, study curriculum and examinations associated with this programme.

Section 2
Objectives of the degree programme and career relevance

(1) The Bachelor's degree programme 'Cybersecurity (English)' is an English-language programme in an international environment that aims to build on the mathematical and scientific foundations of the subject so that graduates are capable of solving problems in the field of cybersecurity. In addition, graduates from the programme are able to address complex questions, including those within a more general context, by applying modern scientific and computer-assisted methods and techniques. Besides the academic training they receive, students also learn the practical and vocational skills that are of relevance in the industrial or commercial sectors. To meet these objectives, students are provided with a solid grounding in the mathematical foundations of the field and in the key concepts and techniques of computer science. The academic and practical training is also complemented by specialist events in the different areas of cybersecurity. Practical skills classes and project work constitute a further important element of the degree programme by providing students with the opportunity to apply the theoretical principles that they have acquired.

(2) The academic training that students acquire in the B.Sc. programme 'Cybersecurity (English)' provides a solid foundation on which to study for a Master's degree in this and related fields.

Section 3
Start and duration of programme

(1) Students begin the programme at the start of the winter semester.

(2) The curriculum is organized such that the programme can be completed in six semesters (standard period of study).

Section 4
Teaching and learning formats

The curriculum content is taught using the following types of academic instruction:

1. Lectures ('L', standard class size = 100): Lectures serve to introduce a particular subject area and also provide an overview of the relevant theoretical concepts and principles, methodologies and skills, technologies and practical implementations that are common to the subject. Lecture courses provide suggestions for further reading on a topic and open the way to acquiring a deeper understanding of an area through subsequent exercise and problem-solving classes, practical skills classes and self-directed study.

2. Exercise and problem-solving classes ('EP', standard class size = 20): Exercise and problem-solving classes are small-group sessions used primarily to supplement and reinforce what was learned in the lectures. Students work on representative problems as this provides an opportunity for them to apply and deepen the knowledge they acquired in the lectures, to assess their personal understanding of a specific area and to clarify any questions that they may have.

3. Seminars ('S', standard class size = 15): Seminars provide an opportunity for students to broaden the knowledge and skills that they have already acquired and to gain a deeper understanding of a particular field of research by participating in discussions, giving presentations or completing seminar assignments based on their study of the specialist literature and relevant academic sources. They also help students acquire the skills necessary for the effective oral and visual presentation of scientific and academic content and encourage students to engage in critical analysis and discussion of research results. A seminar may also include project-related work in areas of current scientific interest or debate. The deeper understanding of a particular field that students acquire through project-related work in the Bachelor's seminar may provide the basis for their Bachelor's thesis project.

4. Practical skills classes and project work ('P', standard class size = 15): Practical skills classes or projects offer a number of practical, subject-related topics that introduce students to the specific approaches and methods used in a particular discipline or field of study. The necessary theoretical knowledge underlying a specific topic is acquired by attending lectures and studying the relevant scientific literature. An additional goal of the practical skills classes is to provide students with the opportunity to gain practical experience with computer-aided methods. Projects tend to address interdisciplinary topics. Working on a topic offers students the opportunity to work in supervised groups to tackle specific assignments from the initial solution design concept through to its final practical implementation. Students learn about the relationships between theory and practice not only through their own independent study and research, but also through project-based teamwork. Participation in a particular practical skills class or project may be dependent on a student having first successfully completed a required course of lectures and the associated exercise and problem-solving classes.

Section 5
The structure and content of the programme

(1) To graduate from the Bachelor's degree programme 'Cybersecurity (English)', students shall earn a total of 180 credits (often referred to in Germany as 'credit points' or 'CPs') as defined by the European Credit Transfer System (ECTS). As a rule, students are required to earn 30 credits per semester.

(2) The degree programme comprises modules from different module categories. Appendix A provides details of the modules and module elements in each of these categories, the type of academic instruction used, the associated workload (number of credit hours per week), the ECTS credits earned, the type of academic assessment and whether the module is graded. Students are required to earn the specified number of credits in each of the module categories. The 'mandatory elective' category comprises modules or module elements that a student can select from a specified list.

1. 18 graded credits from the mandatory area 'Fundamentals of Mathematics':

a) Mathematics for Computer Scientists 1 (9 credits)

b) Mathematics for Computer Scientists 2 (9 credits)

2. 54 graded credits from the mandatory area 'Fundamentals of Computer Science':

a) Programming 1 (9 credits)
b) Programming 2 (9 credits)
c) Fundamentals of Data Structures and Algorithms (6 credits)
d) Introduction to Theoretical Computer Science (9 credits)
e) System Architecture (9 credits)
f) Statistics Lab (6 credits)
g) Elements of Machine Learning (6 credits)

3. 15 ungraded credits from the mandatory practical skills classes:

a) Practical Training 'Software Engineering Lab' (9 credits)
b) Practical Training 'Cybersecurity Lab' (6 credits)

4. 24 graded credits from the specialist mandatory area of cybersecurity:

a) Foundations of 'Cybersecurity 1 (9 credits)
b) Foundations of Cybersecurity 2 (6 credits)
c) Cryptography (9 credits)

5. 5 graded credits from the mandatory elective category 'Introductory Seminars on Topics in Cybersecurity' (each worth 5 credits)

6. 7 graded credits from the mandatory elective category 'Seminars on Topics in Cybersecurity' (each worth 7 credits)

7. At least 12 graded credits from the mandatory elective category 'Core Topics in Cybersecurity' (each typically worth 6 credits per module)

8. At least 12 graded credits from the mandatory elective category 'Complementary Topics in Cybersecurity' (each typically worth 6 credits per module)

9. At least 6 ungraded credits from the mandatory elective category 'German or English

Language Courses' at Saarland University (note: the language chosen shall not be the student's native language); the Examination Board may, on request, permit courses in other languages if the student can demonstrate that they already have a very good command of spoken and written German and spoken and written English.

10. At least 6 ungraded credits from the mandatory elective category 'Freely Selectable Modules', where modules/module elements can be chosen from the following options:

a) Freely selectable modules from the courses offered at the Department of Computer Science, but excluding the core lecture course 'Security'

b) Tutoring and supervising undergraduate students in exercise and problem-solving classes (usually 4 credits). Tutoring several groups of students is permitted, provided that the exercise and problem-solving classes are from different modules.

c) Additional language courses (maximum of 6 credits; modern languages only and not the student's native language).

d) Work placement or internship in industry (maximum of 6 credits) for which an application was submitted to and approved by the Examination Board.

e) Modules / module elements for which an application was submitted to and approved by the Examination Board. Students may, for example, submit an application to the Examination Board requesting recognition of certain student activities (particularly university-related administrative activities) or of attendance at courses teaching key skills (maximum of 3 credits in each case).

11. 9 graded credits from the Bachelor's seminar on topics in cybersecurity or computer science and
12 graded credits for a Bachelor's thesis on a topic in the field of cybersecurity or computer science.

(3) Of the 180 credits that have to be earned in the Bachelor's degree programme 'Cybersecurity (English)', 153 credits shall be from graded assessments or assignments.

(4) To fulfil the requirements of the mandatory sections of the curriculum, students shall complete all of the modules specified in Section 5(2), items 1, 2, 3, 4 and 11 above. (Total number of credits to be earned: 132). In the mandatory elective sections of the programme curriculum, students can take modules or module elements from a specified list, provided that they meet the relevant prerequisites for the particular module or module element selected. (Total number of credits to be earned: at least 48).

(5) The number of places available in practical skills classes, introductory seminars, seminars, tutoring activities and language courses may be limited. Admission to these modules is managed by the module coordinator.

(6) Academic credits are either graded or ungraded. A graded academic assessment or examination cannot be split into ungraded and graded credits.

(7) If a student fails an assessment or examination for a module from Section 5(2), items 1, 2, 3, 4a or 4b above at the first scheduled attempt, the student shall be permitted to retake the assessment or examination on one further occasion within the same examination or assessment period provided that the module completion deadline has not expired (cf. Section 13(4) of the Examination Regulations). In such cases, the first failed attempt shall be treated as if it had not occurred (cf. provisions governing the '*Freiversuch*' option in Section 17(4) of the Examination Regulations). The completion deadline for the aforementioned modules is the end of the sixth

semester.

(8) A student who received academic credits for successfully completing a module as per Section 5(2), items 1, 2, 3, 4a–4c or a core lecture course (cf. Section 5(2), item 10a) is permitted to retake the assessment or examination on one further occasion within the same examination period (cf. Sec. 13(4) of the Examination Regulations) and during the standard period of study in order to attain a better grade. A student who received academic credits for successfully completing an advanced lecture course is permitted to retake the assessment or examination on one further occasion within the same examination period in order to attain a better grade, provided that the lecturer gave notice at the beginning of the course that the final examination or assessment may be repeated for this purpose. The student will be awarded the higher of the two grades. In all other cases, students are not permitted to repeat an assessment or examination for which they have already achieved at least the minimum passing grade.

(9) The modules in the mandatory sections of the programme are offered at least once a year. The modules offered as core lecture courses in the mandatory elective category are offered at least once every two years. Introductory seminars, seminars and modules in the mandatory elective categories ‘Complementary Topics in Cybersecurity’ and ‘Core Topics in Cybersecurity’ will not necessarily be repeated. The Dean of Studies will ensure that a sufficient number of courses and modules are offered in each academic year.

(10) The language of instruction in this degree programme is normally English. Any exceptions will be announced at the beginning of the module or module element.

(11) The range of modules offered as mandatory electives may be modified for one or more semesters, though any such change shall require the approval of the Examination Board. These additional modules or module elements, their weighting in ECTS credits and their classification within the different module categories will be announced before the semester begins.

(12) Detailed information regarding the content of modules and module elements is provided in the module catalogue that will be made available in suitable form. Any changes or amendments to the information in the module catalogue that are not covered by the provisions of these regulations shall be reported to the Dean of Studies and documented appropriately.

(13) Course attendance may be compulsory for certain introductory seminars, seminars, problem-solving classes and practical skills classes. Students will be notified of this by the instructor at the beginning of the module or module element. The compulsory attendance requirement is normally deemed to have been met if a student was present for at least 85% of the course sessions. If there are reasonable grounds for a student’s absence, the student may be offered the option of completing alternative assignments.

(14) Modules that have the same content and that differ only in the language of instruction used shall be treated as a single module with respect to the number of examination attempts permitted and the rules regarding failed first attempts (*Freiversuch* option) and retakes to improve the grade attained, if such provisions are contained in the relevant study regulations.

Section 6
Study plan

The Dean of Studies shall compile a study plan based on these study regulations that includes details of the types and scope of the modules / module elements offered (Appendix A) with

recommendations on how students can organize and structure their studies efficiently (Appendix B). The study plan will be made available in suitable form. The range of modules / module elements offered in the different module categories in a particular semester will be published in the Saarland University course catalogue for that semester.

Section 7
Student advisory services

(1) The Central Student Advisory Service (*Zentrale Studienberatung*) at Saarland University provides counselling and guidance to prospective students and enrolled students concerning the content, structure and requirements of academic study at Saarland University. It can also assist students when deciding between various study options and can provide advice on general questions regarding study planning and organization.

(2) Questions concerning curricular demands, learning objectives, admission requirements and programme-specific study planning and organization can be addressed to the programme adviser with responsibility for the programme 'Cybersecurity (English)'.

(3) Questions specific to individual modules / module elements should be addressed to the respective module coordinators.

Section 8
Study abroad period

Students have the opportunity to spend part of the programme studying abroad. The study abroad period should be taken after the student has completed the modules that cover the fundamentals of the subject. Students interested in studying abroad should seek advice from a relevant source, take preparatory language courses as needed and should clarify credit transfer arrangements in accordance with the examination regulations by completing a study abroad learning agreement. Information on study abroad opportunities, exchange programmes, scholarships and administrative formalities is available from Saarland University's International Office or from the relevant departmental or subject representatives. As foreign host universities and scholarship-awarding bodies often have early application deadlines and long application processing times, study abroad applications should normally be submitted to the Examinations Office one year before the planned start date.

Section 9
Bachelor's thesis and Bachelor's seminar

(1) By completing a Bachelor's thesis, students demonstrate that they are able to work independently on addressing a theoretical-conceptual problem and/or an applied problem in the field of cybersecurity or a related area. The completion period for the thesis is three months. Students are awarded 12 ECTS credits for completing their Bachelor's thesis.

(2) Before finishing their Bachelor's thesis, each student shall have successfully completed a Bachelor's seminar in an area of direct relevance to the topic being addressed in the thesis. Students attending a Bachelor's seminar shall give an oral presentation on the problem they propose to tackle in their thesis project and submit a written description of the issues to be addressed.

(3) Students shall register their thesis project with the Examinations Office no later than one

semester after successfully completing the Bachelor's seminar. Students who fail to meet this deadline will be required to successfully complete another Bachelor's seminar.

Section 10
Commencement

(1) These regulations shall come into force on the day after they are announced in the Official Bulletin of the Institutions of Higher Education in Saarland (*Dienstblatt der Hochschulen des Saarlandes*).

Saarbrücken, 12 August 2021

On behalf of the President of Saarland University
Univ.-Prof. Dr. Manfred Schmitt

Vice-President for Administration and Finance
Dr. Roland Rolles

Appendix A – Modules, assessments and examinations in the Bachelor's degree programme 'Cybersecurity (English)'

Bachelor's degree programme Cybersecurity (English)						**Winter semester**		**Summer semester**		**Winter semester**		**Summer semester**		**Semester break**		**Winter semester**		**Summer semester**	
						Subject semester													
Module category	**Modules**	**Type of assessment**	**Graded/ Un-graded**	**ECTS credits**		**1**		**2**		**3**		**4**				**5**		**6**	
				u	g	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits	L / EP / P hrs/wk	credits
Fundamentals of Mathematics	Mathematics for Comp. Scient. 1	written exam(s), PA	g	0	9	4 / 2 / 0	9												
	Mathematics for Comp. Scient. 2	written exam(s), PA	g	0	9			4 / 2 / 0	9										
Fundamentals of Computer Science	Programming 1	written exam(s), PA	g	0	9	4 / 2 / 0	9												
	Programming 2	written exam(s), PA	g	0	9			4 / 2 / 0	9										
	Data Structures and Algorithms	written exam(s), PA	g	0	6					2 / 2 / 0	6								
	Introduction to Theoretical CS	written exam(s), PA	g	0	9					4 / 2 / 0	9								
	System Architecture	written exam(s), PA	g	0	9							4 / 2 / 0	9						
	Statistics Lab	written exam(s), PA	g	0	6							2 / 2 / 0	6						
	Elements of Machine Learning	written exam(s), PA	g	0	6											2 / 2 / 0	6		
Practical skills classes	Software Engineering Lab	Project work	u	9	0									2 / 0 / 4	9				
	Cybersecurity Lab	Project work	u	6	0					1 / 0 / 3	6								
Cybersecurity	Foundations of Cybersecurity 1	written exam(s), PA	g	0	9	2 / 2 / 2	9												
	Foundations of Cybersecurity 2	written exam(s), PA	g	0	6			2 / 2 / 0	6										
	Cryptography	written exam(s), PA	g	0	9							4 / 2 / 0	9						
Language course (German or English)	(Language course modules, 3 or 6 credits)	oral, written	u	6	0				6										
Introductory seminars on topics in cybersecurity*		oral, written	g	0	5					0 / 0 / 2	5								
Seminars on topics in cybersecurity*		oral, written	g	0	7											0 / 0 / 3	7		
Core Topics in Cybersecurity	(see below)	written exam(s), PA	g	0	12											2 / 2 / 0	6	2/ 2 / 0	6
Complementary Topics in Cybersecurity*	(see below)	written exam(s), PA	g	0	12							2 / 2 /0	6			2 / 2 / 0	6		
Freely selectable modules	(see below)	various	u	6	0		3												3
	Bachelor's Seminar	oral, written	g	0	9														9
	Bachelor's Thesis	Bachelor's thesis (final-year research project and thesis)	g	0	12														12
TOTAL				**27**	**15 3**		**30**		**30**		**26**		**30**		**9**		**25**		**30**

* For a list of the modules currently offered, please go to the Examinations Office website.

Key: L = Lecture, EP = Exercise and problem-solving class, P = Project or practical training, PA = Preliminary assessment, credits = ECTS credits, credit hrs/wk = no. of class or supervised hours per week during the semester, u = ungraded, g = graded

Mandatory elective section: 'Freely selectable modules'				
Tutoring	Tutoring	u	4	0
Language courses (max. 6 credits)	oral, written	u	3 / 6	0
Industrial work placement / internship (max. 6 credits)		u	6	0
Other lecture courses in computer science				
The Examination Board may add modules to or withdraw modules from this list.				

Mandatory elective section: 'Core Topics in Cybersecurity'				
Advanced Public-Key Cryptography	written exam(s), PA	g	0	6
Algorithms in Cryptanalysis	written exam(s), PA	g	0	6
Generating Software Tests	written exam(s), PA	g	0	6
Machine Learning in Cybersecurity	written exam(s), PA	g	0	6
Mobile Security	written exam(s), PA	g	0	6
Obfuscation	written exam(s), PA	g	0	6
Parameterized Verification	written exam(s), PA	g	0	6
Physical-Layer Security	written exam(s), PA	g	0	6
Privacy Enhancing Technologies	written exam(s), PA	g	0	6
Reactive Synthesis	written exam(s), PA	g	0	6
Secure Web Development	written exam(s), PA	g	0	6
Side-Channel Attacks & Defenses	written exam(s), PA	g	0	6
Usable Security	written exam(s), PA	g	0	6
Web Security	written exam(s), PA	g	0	6
The Examination Board may add modules to or withdraw modules from this list.				

Mandatory elective section: 'Complementary Topics in Cybersecurity'				
Automated Debugging	written exam(s), PA	g	0	6
Big Data Engineering	written exam(s), PA	g	0	6
Elements of Statistical Learning	written exam(s), PA	g	0	6
Ethics for Nerds	written exam(s), PA	g	0	6
Concurrent programming	written exam(s), PA	g	0	6
Cybersecurity Laws and Regulations – Legal Aspects of Data Protection	written exam(s), PA	g	0	6
Cybersecurity Laws and Regulations – Legal Aspects of Cybercrime	written exam(s), PA	g	0	6
Topics in Algorithmic Data Analysis	written exam(s), PA	g	0	6
The Examination Board may add modules to or withdraw modules from this list.				

Appendix B

Sample study plan – Bachelor's degree programme Cybersecurity (English)

← Semester					ECTS credits →
1	Programming 1 (9 credits)	Mathematics for Computer Scientists 1 (9 credits)	Foundations of Cybersecurity 1 (9 credits)	Mandatory Elective (e.g. Introduction to Python, 3 credits)	30
2	Programming 2 (9 credits)	Mathematics for Computer Scientists 2 (9 credits)	Foundations of Cybersecurity 2 (6 credits)	Language Course (6 credits)	30
3	Cybersecurity Lab (6 credits)	Introduction to Theoretical Computer Science (9 credits)	Fundamentals of Data Structures and Algorithms (6 credits)	Cybersecurity Introductory Seminar (5 credits)	26
4	Cryptography (9 credits)	System Architecture (9 credits)	Cybersecurity Complementary Lecture (6 credits)	Statistics Lab (6 credits)	30
	'Software Engineering Lab' (9 credits) takes place during break between summer and winter semesters				9
5	Advanced Lecture Course Cybersecurity (6 credits)	Elements of Machine Learning (6 credits)	Cybersecurity Complementary Lecture (6 credits)	Cybersecurity Seminar (7 credits)	25
6	Advanced Lecture Course Cybersecurity (6 credits)	Bachelor's Thesis (12 credits)	Bachelor's Seminar (9 credits)	Mandatory Elective (e.g. language course, 3 credits)	30