fiw.thws

Faculty of Computer Science and Business Information Systems

Technical University of Applied Sciences Würzburg-Schweinfurt

Module Handbook

Bachelor Information Security (B. Sc.)

Summer semester 2025
Winter semester 2025

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Contents

1. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810040
Algebra

Module profile

Exam number
6810040

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Andreas Keller

Lecturer(s)
Prof. Dr. Andreas Keller

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
School maths

Content
General principles:
- Body of real numbers
- Principle of complete induction
- Introduction to the field of complex numbers

Linear algebra:
- Vector spaces (linear independence, basis and dimension)
- Matrices (calculating with matrices, trace and determinant, rank of a matrix)
- Linear systems of equations
- Gaussian algorithm
- Linear mappings

Elementary number theory:
- Residual representation of integers, ggT
- Extended Euclidean algorithm
- Modulo calculus
- Calculating with residue classes
- Linear congruence equations
- Modular exponentiation

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students remember basic mathematical concepts and procedures relevant to computer science.
2. students understand the principles of algebraic and geometric mathematics and their application in computer science contexts.
3. students apply mathematical techniques to solve problems in computer science and develop solution strategies.
4. students analyse mathematical problems and identify suitable solution approaches taking into account various mathematical theories.
5. students evaluate different solution strategies for their efficiency and appropriateness in computer science.
6. students create mathematical models to abstract and solve complex problems in computer science.

Literature
Bartholomé, Andreas; Rung, Josef; Kern, Hans: Number Theory for Beginners. Vieweg+Teubner, Wiesbaden, 2013.
Beutelspacher, Albrecht; Zschiegner, Marc-Alexander: Discrete mathematics for beginners. Vieweg+Teubner, Wiesbaden, 2014.
Gramlich, Günter: Linear Algebra - An Introduction. Fachbuchverlag Leipzig in the Carl Hanser Verlag, 2021.
Hartmann, Peter: Mathematics for computer scientists. Vieweg +Teubner, Wiesbaden, 2020.
Papula, Lothar: Mathematics for Engineers and Scientists Volumes 1 and 2. Vieweg+Teubner, Wiesbaden, 2018.
Pommersheim, James E.; Marks, Tim K.; Flapan, Erica L.: Number Theory: A Lively Introduction with Proofs, Applications, and Stories. John Wiley & Sons. 2010.
Schubert, Matthias: Mathematics for Computer Scientists. Vieweg +Teubner, Wiesbaden, 2012.
Strang, Gilbert: Linear Algebra. Springer-Verlag, Berlin/Heidelberg/ New York, 2003.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5101620,6810030 Databases

Module profile

Exam number
5101620,6810030

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Frank-Michael Schleif

Lecturer(s)
Michael Rott

Applicability	BIN, BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
bZv

Recommended prerequisites for the participation in the module
none

Content
The module teaches the basic concepts and techniques of database development. The relational data model and the relational algebra are introduced as theoretical foundations. One focus is on database modelling, in particular the creation of entity-relationship models (ER models) and their conversion into relational schemas, taking normal forms into account. Introduction to the SQL language, including data manipulation, data queries and the definition of schemas and transaction management. Database development and administration is practised in practical exercises and projects during the semester.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students can explain basic concepts of data persistence and the differences between persistent and non-persistent data.
- Students can define the central terms of relational databases, such as relation, primary key, foreign key and normalisation.
- Students understand relational algebra and can apply simple operations to it.
- Students can explain the connection between conceptual, logical and physical data modelling and justify their significance for database development.
- Students are able to create entity-relationship models (ERM) for given use cases and convert these into relational schemas.
- Students can formulate and execute SQL queries for data manipulation (DML) and schema definition (DDL).
- Students can analyse existing database schemas and evaluate them with regard to redundancy, consistency and normal forms.
- Students are able to analyse technical information requirements and derive suitable data structures and queries from them.

Literature

- Michael Kofler (2024). Database Systems - The Comprehensive Textbook (2nd edition). Bonn: Rheinwerk Verlag GmbH
- Kemper, A., & Eickler, A. (2015). Database systems - An introduction (10th edition). Munich: De Gruyter Oldenbourg Verlag
- Elmasri, R., & Navathe, S. B. (2015). Fundamentals of database systems (7th edition). Munich: Pearson Studium
- Garcia-Molina, H., Ullman, J. D., & Widom, J. (2013). Database Systems: The Complete Book (2nd ed.). Upper Saddle River, NJ: Pearson
- Saake, G., Sattler, K.-U., & Heuer, A. (2011). Databases - Concepts and Languages (3rd ed.). Munich: Pearson Studium

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111010,6810010
Basics of Algorithms and Data Structures

Module profile

Exam number
5111010,6810010

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Frank Deinzer

Lecturer(s)
Prof. Dr. Frank Deinzer,
Prof. Dr. Dominik Seuß

Applicability	BIN, BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Theoretical topics
- Recursion: end-recursive/non-end-recursive, linear recursion/tree recursion
- Complexity: O-notation, runtime complexity, memory complexity
- Higher order functions
- (Anonymous) lambda functions
- Abstraction mechanisms: procedural abstraction, abstraction with data
- Representation of complex data structures
- Sorting and searching

Practical topics
- Numerical algorithms
- Algorithms on lists
- Algorithms on trees
- Algorithms on fields
- Algorithms on symbolic data
- Algorithms on strings
- Algorithms on sets
- Algorithms on queues

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students develop an understanding of the stylistics and aesthetics of programming at the beginning of their training.
Students understand the basic techniques for algorithmic problem solving.
Students generalise the appropriate application of important techniques for mastering complex systems.
Students apply concepts in the areas of recursion and abstraction.
Students apply standard solution techniques to algorithmic problems.

Literature
Abelson, Sussman: Structure and interpretation of computer programs. Springer Verlag, 4th edition, 2014
Wagenknecht: Programming paradigms: An introduction based on Scheme. Vieweg+Teubner, 2013

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810050
Foundations of Information Security

Module profile

Exam number
6810050

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
In this module, topics that are fundamental for further modules in the Information Security degree programme are explained in the necessary technical depth.
The basics of operating systems, applications, computer networks and programming are always taught with a focus on information security issues.
Different types of attackers, their motivation and their business models are discussed using well-known scenarios from the past as examples.
Furthermore, the various job profiles, the associated tasks and possible career options in the field of information security are presented.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students...

- understand the basic protection goals of information security
- know popular strategies of digital attacks, the motivations and/or business models behind them
- understand the functioning of operating systems and their security mechanisms and security problems
- understand the basic sequence of programmes and processes and the associated security-relevant interactions
- know the basics of digital communication, computer networks and the internet
- are familiar with various job profiles and the associated tasks in the field of information security
- can write simple programmes in a scripting language

Literature
Jason Andress, Foundations of Information Security, 2019
Andrew S. Tanenbaum, Modern Operating Systems, 4th edition, 2016
Andrew S. Tanenbaum, Computer Networks, 5th updated edition, 2019
Justin Seitz & Tim Arnold, Black Hat Python, 2nd edition, 2021

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5000130,5100130,6810020 Programming I

Module profile

Exam number
5000130,5100130,6810020

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Steffen Heinzl

Lecturer(s)
Prof. Dr. Steffen Heinzl, Christine Zilker

Applicability	BIN, BISD, BWI
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
bZv

Recommended prerequisites for the participation in the module
none

Content
The Programming I module is about learning procedural programming and the first parts of object-oriented programming in the Java programming language. The ability to programme and thus to independently solve small problems in different areas is one of the basic skills expected of a (business) computer scientist.

The course consists of 13 lessons, which consist of learning videos, the corresponding exercises, the Power Point slides for the videos and quizzes that match the material.

The learning videos are structured in such a way that students gradually familiarise themselves with the various language constructs and basic programming concepts. The accompanying seminar lessons are used to ask questions and consolidate the material.

The exercises are by far the most important part of the course. Students learn programming by solving problems independently. The tutorials help by giving students food for thought from the lecturer if a student gets stuck with a problem and by discussing and improving the quality of solutions. The exercises usually belong to the previous learning videos and pick up on their content.

There is a quiz for each lesson, which uses simple questions to give students the opportunity to check whether they know or understand the material covered.

Contents:
- Introduction/first programme (Hello world)
- Elementary language constructs (expressions, primitive variables, assignments)
- Essential (control) statements (conditional statements, branching, header- and footer-controlled loops)
- Methods, recursion, arrays, complex data types
- Object-orientation (introduction), classes, objects, (instance) methods, visibility
- Multidimensional arrays, behaviour of reference types, string methods, garbage collector

- Data structures (singly and doubly linked lists, binary trees, traversing trees)
- Packages, implicit inheritance, relations using the example of equals
- DRY principle, tell, don't ask principle
- Optional: bitwise operators

- IDE used: Eclipse

This module is the basis for Programming 2 and the programming project. Furthermore, the content and skills acquired in this module make the Programming 3 module much easier and are useful for

- Mathematical SW in computer science
- Algorithms and data structures 2
- Operating systems
- Fundamentals of distributed systems
- Data Management & Data Science

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- apply procedural programming as well as introductory principles of object-oriented programming
- independently implement a solution strategy for writing small procedural and object-oriented Java programmes according to a given design idea
- understand simple mathematical and technical problems and implement a solution
- generalise sub-problems by suitable means

Literature
Heinisch, Cornelia; Müller-Hofmann, Frank; Goll, Joachim: Java als erste Programmiersprache; Vom Einsteiger zum Profi; Springer Vieweg, 2023
Christian Ullenboom: Java ist auch eine Insel, 17th, updated and revised edition, Rheinwerk Computing, 2023
Reinhard Schiedermeier: Programming with Java, Pearson Studium - IT, 2010

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6820020
Programming in Python

Module profile

Exam number
6820020

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Tristan Wimmer

Lecturer(s)
Prof. Dr. Tristan Wimmer, Christine Zilker

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
This module aims to teach students the basics of programming using the Python programming language. It introduces the basic concepts of programming languages and programming paradigms and creates the basis for further modules in the Software Engineering degree programme.
The following topics are covered:

- Elementary data types, data structures and operators
- Control structures: loops and conditional statements
- Programming with functions
- Introduction to object-orientated programming
- Introduction to the concept of inheritance
- Introduction to exception handling

In addition to these topics, this module demonstrates the appropriate structuring options for code, as well as documentation options for a clean and readable programming style. Furthermore, students are shown how best to encounter and solve problems.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to identify and name the basic data types, data structures and operators and apply them in the Python programming language.

- Students will be able to explain how control structures such as loops and conditional statements control the flow of programmes and how these are implemented in Python.
- After successfully completing the module, students will be able to write simple Python programmes that use functions and parameter passing to solve specific tasks, applying the principle of divide and conquer.
- Students will be able to apply object-oriented programming to improve the structure and maintainability of a programme through encapsulation.
- After successfully completing the module, students will be able to design and implement an object-oriented programme in Python for a specific requirement using the basic principles of inheritance.
- After successfully completing the module, students will be able to apply exception handling for incorrect inputs and data type incompatibilities.

Literature
Häberlein, Tobias. Programming with Python: An Introduction to Procedural, Object-Oriented and Functional Programming. 1st ed. 2024. Berlin, Heidelberg: Springer Berlin Heidelberg, 2024. https://doi.org/10.1007/978-3-662-68678-2.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810060
Social Engineering and Security Awareness

Module profile

Exam number
6810060

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Andreas Schütz

Applicability	BISD
Semester according to SPO	1. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
The module Social Engineering and Security Awareness focuses on the human factor of information security. People make a decisive contribution to information security in companies with their behaviour - they are an important security factor. Due to this influence, they are increasingly targeted by cyber criminals. The module primarily looks at these two aspects - security factor and victim - of the human factor in information security.

Information security awareness describes the sensitisation of employees for information security (security factor). The module contains the following contents on awareness:
- Concept and models, psychological understanding of awareness
- Practical examples of awareness measures
- Promoting and measuring awareness

Social engineering is the targeted manipulation of people in order to seduce them into unintentional actions (victims). The following contents, among others, are dealt with in social engineering:
- Basics and forms
- Psychological tricks
- Phishing and phishing simulations

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students see people as a solution and not as a problem for information security.
They explain the role of the human factor in information security using examples.
The students know and identify the principles of social engineering and can explain them using examples.
They name different forms of phishing and can discuss the advantages and disadvantages of phishing simulations.
They understand what information security awareness means and know methods to enhance the different aspects of awareness.
Students can create awareness measures in a targeted and individualised way.

Literature
Beißel, S.: Security Awareness, De Gruyter, 2019.
Cialdini, R.: Influence - The Psychology of Persuasion, Collins Business, 2007.
Hadnagy, C. (with Schulman, S.): Human Hacking - Win Friends, Influence People, and Leave Them Better off for Having Met You, Harper Business, 2021.
Helisch, M.; Pokoyski, D. (eds.): Security Awareness - New Ways to Successfully Sensitise Employees, Vieweg+Teubner, 2010.
Schroeder, J.: Advanced Persistent Training, Apress, 2017.
Verplanken, B. (Ed.): The Psychology of Habit - Theory, Mechanisms, Change, and Context, Springer, 2018.
Weber, K.: Humans and Information Security, Hanser, 2024.
Weber, K.; Schütz, A.; Fertig, T.: Fundamentals and Application of Information Security Awareness, SpringerVieweg, 2019.
Take Aware Sec&Life Magazine, https://www.take-aware-events.com/news-post/magazinesecandlife

2. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 9999999
General Compulsory Elective

Module profile

Exam number
9999999

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Jochen Seufert

Lecturer(s)
Beate Wassermann

Applicability	BEC, BDGD, BISD
Semester according to SPO	2. semester
Type of module	AWPM

Required prerequisites for the participation in the module according to the SPO
As a rule, none; exceptions are determined and announced by the Faculty of Natural Sciences and Humanities.

Recommended prerequisites for the participation in the module
none

Content
Selection of two general science electives (AWPF) (2 x 2 SWS) or one AWPF (1 x 4 SWS) from the range of subjects offered by the Faculty of Applied Natural Sciences and Humanities (FANG).

Range of subjects offered by the FANG in the areas of
- languages
- cultural studies
- Natural sciences and technology
- Politics, law and economics
- Education, psychology and social sciences
- Soft skills
- Creativity and art.

Courses whose content is already part of or directly related to parts of other modules of the degree programme are excluded from the FANG catalogue. The corresponding courses are marked with a blocking note in the FANG subject catalogue.
The contents of the individual AWPFs are published on the FANG faculty's own homepage.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
The subject-specific learning objectives depend on the AWPF selected.
The students

- also acquire knowledge and competences that are not subject-specific but may be important for the desired career goal, such as special knowledge of foreign languages, natural sciences or social sciences
- analyse a wide variety of issues
- categorise subject-specific knowledge in an interdisciplinary context
- transfer what they have learnt to their current training
- have expanded their key competences and, where applicable, foreign language skills, which supports their personal development, also in intercultural terms
- are aware of their personal, social and ethical responsibilities.

Literature
depending on the selected AWPFs

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810100
Basics of Cryptography

Module profile

Exam number
6810100

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Andreas Keller

Lecturer(s)
Prof. Dr. Andreas Keller

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Module "Algebra"

Content
- Mathematical basics
- Block ciphers
- DES and AES
- The RSA method
- Cryptographic hash function
- Discrete logarithms and the ElGamal method

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- name mathematical concepts of number theory and linear algebra that are relevant to cryptographic procedures.
- describe and differentiate between basic cryptographic methods such as symmetric and asymmetric encryption.
- explain the functionality of selected cryptographic algorithms (e.g. RSA, Diffie-Hellman, AES) using mathematical principles.
- analyse the security of cryptographic procedures using mathematical criteria (e.g. prime factorisation, discrete logarithm).
- critically evaluate the applicability of cryptographic methods with regard to key lengths, computational effort and known attack scenarios.
- recognise and explain the limits of cryptographic methods, especially with regard to theoretical and practical attacks.
- work on cryptographic tasks independently and in a structured manner.
- use logical thinking to develop suitable solutions for cryptographic problems and justify them mathematically.
- reflect on the importance of mathematical structures for the security of encryption methods.

Literature
Beutelspacher, Wolfenstetter: Cryptography in Theory and Practice, Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH, Wiesbaden 2010
Delf, Knebl: Introduction to Cryptography, Springer Berlin, Heidelberg, 2016
Ertel: Applied Cryptography, Hanser Verlag, 2018

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810120
ISM-Standards and Processes

Module profile

Exam number
6810120

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Prof. Dr.-Ing. Tobias Fertig

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Social Engineering and Security Awareness

Content
The module Information Security Management (ISM) Standards and Processes deals with the holistic design of information security management in companies and organisations. Information security does not only mean implementing technical measures to protect the IT infrastructure. Rather, organisational, technical, physical and personnel security measures must be coordinated with each other and with the objectives of the organisation. Effective security concepts are developed, implemented, audited, and continuously improved on the basis of established frameworks, taking into account effectiveness, usability and cost efficiency.

Against this background, the module ISM Standards & Processes covers, among others, the following topics:

- Structure and content of information security management (ISM) standards and frameworks (e.g., ISO27001, BSI IT-Grundschutz, CISIS12)
- Creation of holistic information security concepts
- Organisational security measures, e.g., guidelines for information security, classification concept for information
- Metrics and maturity models for information security
- Incident response and business continuity management
- Audits of security concepts and measures

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students know the content and structure of ISMS standards and frameworks and select these depending on the situation.
Students create organisational security measures such as information security guidelines.
Students adapt processes such as incident response and business continuity management to organisation-specific requirements.
Students understand the relationship between effectiveness, efficiency, and usability for the selection and implementation of information security measures.
Students know concepts for the evaluation, auditing, and continuous improvement of ISMS.

Literature
Harich, T.: IT Security Management - Practical Knowledge for IT Security Managers, 2nd Ed., mitp, 2018
Harkins, M.: Managing Risk and Information Security - Protect to Enable, 2nd Ed., Apress, 2016
Kersten, H. et al: IT Security Management according to the new ISO 27001 - ISMS, Risks, Indicators, Controls, 2nd ed, Springer Vieweg, Wiesbaden, 2020
Lang, M.; Löhr, H: IT Security - Technologies and Best Practices for Implementation in Companies, HANSER, 2022
Sowa, A.: Management of information security - control and optimisation, Springer Vieweg, Wiesbaden, 2017
Weber, K.: People and information security, Hanser, 2024.
Whitman, M.; Mattord, H.: Management of Information Security, Cengage Learning, 6th ed., 2018

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111120,6810070
Internet Communication

Module profile

Exam number
5111120,6810070

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christian Bachmeir

Lecturer(s)
Prof. Dr. Christian Bachmeir

Applicability	BIN, BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Rough structure:
1) Introduction to communication networks
2) Theoretical basics of communication technology
3) Practical basics of Internet communication
4) Introduction to IT security
5) Basics of cryptography

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
1. students remember the basic concepts of communication systems on the Internet and their technical foundations.
2. students understand the functioning of wireless communication technology and its effects on data transmission.
3. students apply modern cryptographic methods to ensure the security of Internet communication.
4. students analyse the performance, possibilities and limitations of communication systems on the Internet in order to make well-founded decisions when developing distributed systems.
5. students understand and evaluate the necessity of cryptographic procedures in different application scenarios of everyday operations.
6. students create concepts for the implementation of security mechanisms in Internet communication systems based on cryptographic techniques they have learnt.

Literature
Patrick Schnabel, Communication Technology Primer, Kindle eBooks
Kurose, Ross: Computer Networks, The Top-Down Approach, Publisher: Pearson Studium; Edition: 6th, updated edition, 2019
Tanenbaum, Wetherall: Computer Networks, Publisher: Pearson Studium; Edition: 5th, updated edition, 2013
Schmeh: Cryptography: Methods - Protocols - Infrastructures (iX-Edition) Publisher: dpunkt.verlag GmbH; Edition: 5th, updated edition, 2013

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810110
Penetration Testing

Module profile

Exam number
6810110

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students learn about the profession of penetration tester or security researcher with the associated framework conditions and procedures. In this context, the focus is on identifying, understanding and exploiting common vulnerabilities in IT systems.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- describe the job description of penetration testers or security researchers and explain their tasks in the context of IT security.
- systematically describe the typical process of a penetration test - from information gathering to reporting.
- name the legal framework and ethical aspects of penetration tests and take them into account when carrying them out.
- recognise and practically exploit common vulnerabilities in web applications, classic applications, protocols and hardware components.
- Identify vulnerabilities with common tools (e.g. Burp Suite, Metasploit) and assess their impact in a technically sound manner.
- Apply post-exploitation techniques to extend or deepen access to systems (e.g. credential dumping, privilege escalation).
- describe and exemplify methods of lateral movement in order to move within a network.
- assess and prioritise identified vulnerabilities in terms of their risk potential (e.g. using CVSS).
- document the results of a penetration test in a structured report and present them to the target group.
- reflect on the limits and risks of penetration testing, particularly with regard to unintended effects and liability issues.

Literature
The Web Application's Hackers Handbook (Dafydd Stuttart et al.), 2023
Penetration Testing - a Hands-On Introduction to Hacking (Georgia Weidman), 2014
Hacking, The Next Generation (Nitesh Dhanjani et al.), 2021

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5000220,5100220,6810080 Programming II

Module profile

Exam number
5000220,5100220,6810080

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Steffen Heinzl

Lecturer(s)
Prof. Dr. Steffen Heinzl, Christine Zilker

Applicability	BIN, BISD, BWI
Semester according to SPO	2. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
bZv

Recommended prerequisites for the participation in the module
Programming I

Content
The Programming II module is about learning object-oriented programming (in the Java programming language). In order to structure larger information systems, it is important to learn how these can be structured, designed and tested.

This course consists of 13 lessons, which are made up of learning videos, the corresponding exercises, the Power Point slides for the videos and quizzes matching the material.

The learning videos are structured in such a way that students are first confronted with tests and then gradually learn object-orientation and its application. The accompanying seminar lessons are used to ask questions and consolidate the material.

The exercises are by far the most important part of the course. Students learn object-orientated programming by solving problems independently. The tutorials help by giving students food for thought from the lecturer if a student gets stuck with a problem and by discussing and improving the quality of solutions. The exercises usually belong to the previous learning videos and pick up on their content.

There is a quiz for each lesson, which uses simple questions to give students the opportunity to check whether they know or understand the material covered.

Contents:
Unit tests (JUnit 5)
Dependency management (Maven)
Inheritance (specialisation, generalisation)
Enumerations
Abstract classes, interfaces, composition
Exceptions
streams
generics
Collections, associative arrays (maps)
Nested classes (static nested, inner, local, anonymous classes)
Lambda expressions
Threads

Design patterns: Builder, Decorator, Visitor
Fluent interfaces
Functional programming with the help of the Stream API

IDE: Eclipse or IntelliJ

The content and skills acquired in this module make the Programming 3 and Programming Project modules much easier and are useful for

- Mathematical SW in computer science
- Algorithms and data structures 2
- Operating systems
- Fundamentals of Distributed Systems
- Data Management & Data Science

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- apply the concepts of object-oriented programming
- independently implement a solution strategy for writing object-oriented Java programmes
- implement partial solutions to larger programmes/problems
- structure problems into several sub-problems
- Implement tests for software systems
- Understand and use polymorphism in methods and types
- use class libraries to extend programmes
- understand first design patterns

Literature
Schiedermeier, Reinhard: Programming with Java. Pearson, 2nd edition, 2010.
Schiedermeier, Reinhard: Programming with Java II. Pearson, 2013.
Bloch, Joshua: Effective Java. 3rd Edition, Addison-Wesley, 2017.
Ullenboom, Christian: Java ist auch eine Insel. 16th edition, Rheinwerk Computing, 2021.

3. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111160,6810140
Backend Systems

Module profile

Exam number
5111160,6810140

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 30 hrs

Self-study: 120 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BIN, BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
Programming 1 and Programming 2

Content

- Introduction to distributed systems, client-server, and peer-to-peer systems.
- Software architectures for backend systems (3-tier, hexagonal, monolithic vs. micro-service, event-driven)
- Frameworks to implement backend systems (e.g. Spring)
- Advanced database techniques, scalability, replication, sharding, ORM-tools, query caching, CAP theorem
- Protocols for remote procedure call, for example, GraphQL and Google RPC.
- Basics of the HTTP protocol and application in the form of Web APIs.
- Comprehensive introduction to the REST architecture principle: resources, URLs, CRUD, hypermedia, caching, security.
- Configuration of Web servers (Apache), load balancer, and public caches (nginx)
- Testing of backend systems, performance testing using JMeter, monitoring and logging
- Security aspects of network protocol and backend systems

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the fundamental concepts and differences of distributed systems, including their architecture and communication models.
- The students analyse various software architectures for backend systems and evaluate their suitability for different use cases.
- The students apply advanced database techniques such as replication and sharding to enhance data availability and performance.
- The students implement a backend system using a framework like Spring, following best practices for configuration, deployment, and security.
- The students compare different protocols for remote procedure calls, such as GraphQL and Google RPC, assessing their strengths and limitations.
- The students design RESTful APIs by applying the principles of the REST architecture, focusing on resources, URLs, CRUD operations, and security strategies.
- The students evaluate the security aspects of network protocols and backend systems, proposing improvements based on best practices.

Literature

- Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems: Concepts and Design (4th Edition) (International Computer Science). Boston, MA, USA: Addison-Wesley Longman Publishing Co, Inc, 2005.
- N. Biswas, Practical GraphQL: Learning Full-Stack GraphQL Development with Projects. Berkeley, CA: Apress, 2023.
- J. Webber, S. Parastatidis, and I. Robinson, REST in practice: hypermedia and systems architecture, 1st ed. in Theory in practice. Beijing Cologne: O'Reilly, 2010.
- L. Richardson and M. Amundsen, RESTful Web APIs, First edition, Second release. Beijing Cambridge Farnham Cologne Sebastopol Tokyo: O'Reilly, 2015.
- I. Dominte, Web API Development for the Absolute Beginner: A Step-by-step Approach to Learning the Fundamentals of Web API Development with .NET 7. Berkeley, CA: Apress, 2023.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810180
Governance, Risk, Compliance and Ethics

Module profile

Exam number
6810180

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Prof. Dr. Markus Oermann

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
ISM Standards & Processes

Content
Many people and units inside and outside organisations are involved in the management of information security. Governance regulates how transparency, accountability and efficiency are ensured by defining structures, responsibilities and framework conditions, while at the same time safeguarding the interests of all stakeholders. This module shows which stakeholders are involved in information security management, how responsibilities are defined, decisions are made and optimal framework conditions for maximum information security are created.

The identification and assessment of IT risks helps organisations to deal with threats to information security in a targeted and structured manner. The risk-oriented approach is pursued in many ISMS frameworks (information security management system). The module teaches the basics of IT risk management, such as measures for identifying, analysing, assessing and handling IT risks in a structured risk management process.

In the section on ethics, essential conceptual foundations of moral philosophy are explained. On the basis of established schools of ethics, the normative justification of (information) security as a value and guiding principle is examined. The consideration of models for the integration of ethical considerations in development and system design processes builds a bridge to the application of ethical principles in practice. Questions of compliance with the applicable data protection law are also of particular relevance here. After an overview of its basic structures, the focus is on the requirements for technical and organisational data protection as well as the enforcement and consequences of legal violations. Finally, the basics of the reformed information security law are explained.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- name and specifically design basic governance mechanisms (e.g. responsibilities, guidelines, decision-making processes, committees) in the context of information security.
- describe relevant roles and stakeholders in information security management within and outside of organisations and differentiate between their tasks.
- explain the importance and function of IT risk management for information security and illustrate this using practical examples.
- identify and describe the organisational framework conditions for effective IT risk management.
- understand, apply and document a simple, structured IT risk management process.
- recognise ethical challenges in dealing with digital systems with security relevance and develop solutions for integrating ethical principles into work processes.
- explain the basic structures of data protection law and answer fundamental questions about data protection compliance.
- describe the main contents of information security law and assess their relevance for operational practice.
- communicate in a targeted manner with legal or regulatory experts on issues relating to data protection and information security law.
- reflect on the relationships between governance, risk and compliance management and ethics in security-critical IT environments.

Literature
Harich, T.: IT-Sicherheitsmanagement: das umfassende Praxis-Handbuch für IT-Security und technische Datenschutz nach ISO 27001. 3rd edition, MITP, 2021.
Johannsen, A.; Kant, D.: IT Governance, Risk and Compliance Management (IT-GRC) - A competence-orientated approach for SMEs. In: HMD - Praxis der Wirtschaftsinformatik, 57, 2020, pp. 1058-1074. https://doi.org/10.1365/s40702-020-00625-8
Kersten, H. et al: IT security management according to the new ISO 27001 - ISMS, risks, indicators, controls. 2nd, updated edition, SpringerVieweg, 2020.
Lang, M.; Löhr, H.: IT-Sicherheit - Technologien und Best Practices für die Umsetzung in Unternehmen. 2nd, revised edition, Hanser, 2024.
Lewinski/Rüpke/Eckhardt (2022): Data protection law. 2nd edition. Munich, C.H. Beck.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003230,6810160
IT Project Management

Module profile

Exam number
5003230,6810160

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr.-Ing. Anne Heß

Lecturer(s)
Prof. Dr. Eva Wedlich,
Prof. Dr.-Ing. Anne Heß

Applicability	BISD, BWI
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
- Introduction to project and project management
- Project organisation
- Project planning process
- Project costing
- Project control and monitoring
- Project completion
- Personnel management and project marketing
- IT product management
- Core activities in IT projects (analysis, design, implementation, integration and stabilisation)
- Quality management and quality assurance
- Configuration management (rudimentary)
- Process models (phase models vs. iterative / incremental / agile process models)
- Agile project management / Scrum

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes

- Students learn project management skills, in particular the necessary knowledge for project managers. Project management methods, processes and tools are covered.
- Students are familiarised with relevant core activities of software development and their objectives
- Students can assign and describe relevant sub-activities, input requirements and result types to the core activities
- Students can describe various process models (waterfall model, V-model, Scrum), including their respective advantages and disadvantages, and can describe and assign activities in the process models
- Students understand characteristic features and differences between phase-orientated process models and iterative/ incremental process models and can select suitable process models for a given project context and justify their selection
- Students know the basic principles, roles, artefacts, ceremonies and practices of agile projects (using Scrum as an example) and can find their way around an agile project as a team member
- Students understand the importance and relevance of software quality
- Students know the key concepts of quality management and quality assurance and can describe the relevant tasks and skills (soft skills) of quality managers
- Students know the main objectives, concepts and activities of configuration management, including the basic functionalities of tools to support configuration management

Literature

- Johannsen, A. and Kramer, A.: Basiswissen für Softwareprojektmanager, dpunkt.verlag, 2017.
- Olfert, K.: Projektmanagement, NWB Verlag, 11th edition 2019.
- Sterrer, C. and Winkler, G.: setting milestones. Project management (methods, processes, tools), Goldegg Verlag, 2010.
- Sterrer, C.: pm k.i.s.s.: Keep it short and simple, Goldegg Verlag, 2011.
- Tiemeyer, E: Handbuch IT-Projektmanagement, Hanser 2018
- Ziegler, Michael : Agile project management with Scrum for beginners, ISBN-13: 979-8751100346 , 2021
- Gundlach, Marco: Agile Project Management - Successfully Navigating with Scrum and Kanban: A Comprehensive Guide for Beginners and Experts, ISBN-13: 979-8392911936, 2023

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810170
Security Engineering

Module profile

Exam number
6810170

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Sebastian Biedermann

Lecturer(s)
Prof. Dr. Benjamin Weggenmann,
Prof. Dr. Minal Moharir

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students acquire knowledge and skills for designing and analysing secure IT systems using modern cryptographic methods. The focus is on the practical application of basic cryptographic concepts such as symmetric and asymmetric encryption as well as hashing algorithms for the development of secure applications. In addition, students deal with the functionality and security-relevant aspects of central protocols such as TLS, PGP, Kerberos, VPN/IPSec and the anonymisation network TOR. Current developments such as post-quantum cryptography (e.g. Merkle Signature Scheme), zero-knowledge proofs as well as biometric and multi-factor authentication methods are also covered. Another focus is on the principle of "security by design" and the systematic identification of security-critical vulnerabilities in system architectures. Students learn to analyse security-relevant requirements and use them to design robust (distributed) systems in accordance with current standards. The module thus teaches both conceptual and technical skills for developing secure information systems in complex environments.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After completing the module, students will be able to

- Describe basic cryptographic concepts (e.g. symmetric/asymmetric encryption, hashing) and use them specifically in security-relevant application scenarios.
- explain the functionality of security-relevant protocols such as TLS, Kerberos, VPN/IPSec, PGP or TOR and analyse security-critical vulnerabilities.
- assess modern authentication methods such as multi-factor authentication, biometric methods and their security-related strengths and weaknesses.
- explain the basics of current cryptographic developments such as post-quantum cryptography (e.g. Merkle Signature Scheme) and assess their potential.
- analyse requirements for secure (distributed) systems and systematically translate them into a secure system design.
- Integrate cryptographic procedures into the design of secure systems and protocols, taking into account current standards and best practices.
- recognise potential threats in the design of security-relevant systems and design suitable technical countermeasures.
- Systematically consider and evaluate security properties (e.g. confidentiality, integrity, authenticity) in system designs.
- reflect on the relationship between technical implementation, cryptographic principles and secure system design.

Literature
Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson, 2020
Applied Cryptography: Protocols, Algorithms and Source Code in C, Bruce Schneider, 1996
Bulletproof TLS and PKI, Second Edition: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications, Ivan Ristic, 2022

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003031
Software industry, education and economy in India

Module profile

Exam number
5003031

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Isabel John

Lecturer(s)
Prof. Dr. Isabel John,
Prof. Dr.-Ing. Erik Schaffernicht

Applicability	BDGD, BEC, BIN, BISD, BWI
Semester according to SPO	3. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
Good knowledge of English

Recommended prerequisites for the participation in the module
none

Content
Introduction to India and our partner university Christ University in Bangalore
Selection of topics for the intercultural presentations (e.g. politics, religion, IT industry) in preparation for the excursion.
Presentation of methods for developing presentations in terms of topic selection, structure and slide design.
Introduction to the topic for the joint projects with Christ University students, which will be worked on in small groups from October.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Students recall basic facts about India and its importance in information technology.
Students analyse and evaluate differences between Germany and India.
Students use an image-orientated, free presentation style in their presentations.
Students apply basic communication techniques in the intercultural field using India as an example.
Students demonstrate successful co-operation with students from the partner university in the context of a technical project.

Literature
Will be announced in the seminar depending on the topics.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111140,6820130 System-oriented Programming

Module profile

Exam number
5111140,6820130

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BIN, BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
Programming I and Programming II

Content

- Definition and meaning of system-oriented programming
- Using the command line of an operating system
- Shell programming using the example of Bash
- Data processing on the command line with sed, awk, sort, jq
- Using AI assistance systems (e.g. GitHub Copilot, ChatGPT)
- Editing text documents with vim
- Version control system Git
- Introduction to the C programming language (syntax, data types, pointers, memory management)
- System programming under Linux (system calls, handling files, processes)
- Security aspects of system-related programming and protection mechanisms
- Structure of the Linux operating system
- Processes, process management, scheduling
- Inter-process communication, race conditions, deadlocks, semaphores, Petri nets and deadlock detection, philosopher problem, producer-consumer problem
- Memory management, memory abstraction, partitioning, fragmentation, free memory management, virtual memory, page exchange algorithms
- Input and output, direct memory access, interrupts, hard disks, file systems for hard disks
- Network communication and implementation of network protocols
- Hypervisor technologies, Docker containers, resource management

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the definition and principles of system-oriented programming, including its role in software development.
- The students demonstrate proficiency in using the command line of an operating system, applying advanced tools like sed, awk, sort, and jq for data processing tasks.
- The students develop shell scripts in Bash to automate system tasks and streamline operations effectively.
- The students utilize AI assistance systems, such as GitHub Copilot and ChatGPT, to improve coding efficiency and solve programming challenges.
- The students manage text documents using the vim text editor, employing advanced editing and configuration techniques.
- The students implement version control practices with Git to support collaborative software development workflows.
- The students program in C, focusing on syntax, data types, pointers, memory management, and use debugging and profiling tools like gdb, strace, ltrace, and gprof to analyse code performance.
- The students evaluate security aspects of system-related programming and apply protection mechanisms to ensure code security.

Literature

- D. J. Barrett, Efficient Linux at the command line: boost your command-line skills, First edition. Sebastopol, CA: O'Reilly, 2022.
- A. S. Tanenbaum and H. Bos, Modern operating systems, 4th ed. Boston: Prentice Hall, 2015.
- K. Hitchcock, Linux System Administration for the 2020s: The Modern Sysadmin Leaving Behind the Culture of Build and Maintain. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-7984-7.
- M. Kalin, Modern C Up and Running: A Programmer's Guide to Finding Fluency and Bypassing the Quirks. Berkeley, CA: Apress, 2022. doi: 10.1007/978-1-4842-8676-0.
- K. Hitchcock, The Enterprise Linux Administrator: Journey to a New Linux Career. Berkeley, CA: Apress, 2023. doi: 10.1007/978-1-4842-8801-6.
- J. Varma, Pro Bash: Learn to Script and Program the GNU/Linux Shell. Berkeley, CA: Apress, 2023. doi: 10.1007/978-1-4842-9588-5.
- S. M. Palakollu, Practical System Programming with C: Pragmatic Example Applications in Linux and Unix-Based Operating Systems. Berkeley, CA: Apress, 2021. doi: 10.1007/978-1-4842-6321-1.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810150
Business and IT Law

Module profile

Exam number
6810150

Duration
1 semester

Frequency
Every winter semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Oliver Ehret

Lecturer(s)
Prof. Dr. Oliver Ehret

Applicability

Applicability	BISD
Semester according to SPO	3. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
General contract law
Special contract law with regard to IT, special types of contracts Basic principles of copyright law
Overview of relevant areas of intellectual property law Internet law
Data protection law

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Categorise law, basic legal concepts of our legal system and its basic structures; provide an overview of the role that law plays for IT specialists. Understand the basic principles of general private and public law; understand and classify IT law terms; gain an overview of the main IT-relevant legal areas and contractual areas; recognise, assess and limit legal risks; develop practical skills in dealing with IT-relevant legal problems and know basic types of contracts in the IT sector; acquire basic knowledge of copyright law, especially in the area of software and databases; understand the principles of data protection, especially in the IT sector.
The importance of data protection law, especially in an international context, is emphasised. Emphasis is also placed on conveying how closely computer science, the architecture of IT systems, information security and data protection are interlinked.

Literature
Köhler, Bürgerliches Gesetzbuch, dtv, 89th edition 2022
Schneider: IT and computer law, 15th edition, Beck dtv, Munich 2022.
Kallwass, Abels: Private Law, Verlag Franz Vahlen Munich, 24th edition, 2021
Hoeren: IT Contract Law, 2nd edition, Verlag Otto Schmidt, Cologne 2012.
Marly: Praxishandbuch Softwarerecht, 7th edition, C.H.Beck, Munich 2018.
Härting: Internetrecht, 7th edition, Verlag Otto Schmidt, Cologne 2022.
Hoeren: Skript Internetrecht Uni Münster, as of April 2020
Haug: Basic knowledge of internet law, Verlag W. Kohlhammer, 3rd edition, 2016
Redeker: IT law, C.H.Beck, 7th edition, 2020
Schneider: Handbook, IT law, Otto Schmidt, 5th edition, 2017
Kühling, Sack, Hartmann: Data protection law, 5th edition C.F.Müller, 2021

4. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810240
Expertise and Communication

Module profile

Exam number
6810240

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 30 hrs

Self-study: 120 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr. Kristin Weber

Lecturer(s)
Prof. Dr. Kristin Weber,
Prof. Dr.-Ing. Sebastian Biedermann

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
Module 6810060

Recommended prerequisites for the participation in the module
none

Content
In this seminar, students work independently on current topics from all areas of information security and related topics, such as data protection. The lecturers provide a selection of topics from which the students choose a topic or suggest a different topic. The chosen topic is worked on independently by the students comprehensively and according to scientific principles and documented in a term paper. The accompanying seminar teaches writing and creativity techniques as well as the basics of academic research and work. In addition, students present their topics in a presentation for a non-specialist audience in order to test their ability to present technical topics in a way that is appropriate for the target group.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
After successfully completing this module,

- students will know how to familiarise themselves independently with information security topics and expand their knowledge.
- be familiar with other current issues relating to information security and related topics, e.g. data protection.
- are able to apply the basics of scientific work.
- are able to show, document and discuss interim results and know what role feedback plays in scientific discourse.
- are able to produce a written paper that fulfils scientific standards.
- are able to prepare, communicate and present scientific and technical topics in a way that is appropriate for the target group.
- know writing and creativity techniques and can apply them depending on the situation.

Literature
Aengenheyster, S.; Dörr, K. (eds.): Practical Handbook of IT Communication. SpringerGabler, 2019.
Kirchem, S.; Waack, J.: Personas entwickeln für Marketing, Vertrieb und Kommunikation - Grundlagen, Konzept und praktische Umsetzung. SpringerGabler 2021.
Lubienetzki, U.; Schüler-Lubienetzki, H.: Was wir uns wie sagen und zeigen - Psychologie der menschlichen Kommunikation. Springer, 2020.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5111230,6810200
Frontend Systems

Module profile

Exam number
5111230,6810200

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BIN, BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Backend Systems

Content

- Introduction to Web Technologies: Basic building blocks of web development, including HTML for structuring web content, CSS for styling and layout, and JavaScript for adding interactivity and dynamic behaviour to web pages.
- Advanced JavaScript and Modern ES6+ Features: More details about JavaScript, exploring modern ES6+ features such as let, const, arrow functions, template literals, modules, promises, and async/await, and learn how to apply these in real-world scenarios.
- Fundamentals of React: Core concepts of React, including its component-based architecture, JSX syntax, and the use of state and props to manage data within components, enabling the creation of dynamic and interactive user interfaces.
- Advanced React Techniques: Advanced topics in React, such as the Context API for state management across the application, React hooks for managing state and side effects in functional components, and performance optimisation strategies.
- IT Security in Frontend Development: Principles of IT security as they relate to frontend development, including securing user input, preventing cross-site scripting (XSS) and cross-site request forgery (CSRF), and ensuring secure communication between frontend and backend systems. Introduction to the Open Web Application Security Project Top Ten list.
- Project Development and Deployment: Setting up development environments, following best practices in code organisation and documentation, and deploying and maintaining frontend applications in a production environment.

In the traditional degree programme, the lecturer provides or agrees with the topics of the practical examples for the examination. In the BIN dual study programme, the lecturer consults with the company on a task, ensuring practical relevance and feedback from the company.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes

- The students understand the foundational principles of HTML, CSS, and JavaScript to build and style basic web pages effectively.
- The students apply modern web frameworks like React and Svelte to develop dynamic and responsive user interfaces.
- The students analyse different state management techniques, such as React hooks and the context API, to manage complexity in web applications.
- The students design cross-platform mobile user interfaces using Flutter, focusing on user experience and performance.
- The students implement best practices in frontend development, including version control, testing, and secure deployment processes.
- The students create a comprehensive frontend project from scratch, integrating all learned concepts into a fully functional application.
- The students evaluate different frameworks and tools for frontend development to make informed decisions based on specific project requirements.

Literature

Marijn Haverbeke: Eloquent JavaScript: A Modern Introduction to Programming. 4th edition, 2024.
Alex Banks, Eve Porcello: Learning React: Modern Patterns for Developing React Apps. O'Reilly, 2020.
Thomas Bailey, Alessandro Biessek: Flutter for Beginners: Cross-platform mobile development from Hello, World! to app release with Flutter 3.10+ and Dart 3.x. Packt, 2023.
Andrew Hoffman: Web Application Security: Exploitation and Countermeasures for Modern Web Applications. O'Reilly, 2024.

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6100930,6810190
Innovation Management and Entrepreneurship

Module profile

Exam number
6100930,6810190

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Michael Müßig

Lecturer(s)
Prof. Dr. Michael Müßig

Applicability	BEC, BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Intro: Motivation, innovation, company, founding a company, startup and a look at economic history
Definitions: Management, ... and all terms relating to innovation and types of innovation
Processes and correlations: Adoption and diffusion, acceptance
Prediction: Gartner's hypecycle and the three horizons
Innovation in the company, Schumpeter and the innovator's dilemma, disruption
Startup ecosystems
End-to-end: design thinking, personas and value proposition, business model canvas, lean startup and customer development, MVP and prototyping
The business plan, founding team
Growth and change, growth hacking
Founding, financing, designing and evaluating companies
Open and crowd innovation, Jugaad, frugal and sustainability in founding and innovation

CASE studies (alternating): Tesla, Kodak and digital photography, Fashion and TEC, Scoutbee, Vogel Communications

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- Present and explain the terminology in the field of innovation management as well as business creation and management
- assess statements on regional and company-internal ecosystems for innovation and intra- and entrepreneurship
- Understand the importance of teams and team processes in the field of innovation development and business creation and be able to apply team-building methods
- Students learn the basics of a business plan in terms of its structure and creation and are able to develop and create one independently
- Identify the key tax, legal and economic building blocks of a successful business start-up and analyse their significance
- They will be able to present and design their own business model ideas using the methodical approaches of design thinking, value proposition and business modelling

Literature
Mandatory:
Hess, Thomas: Strategically managing digital transformation. Springer Fachmedien Wiesbaden GmbH, 2019
Osterwalder, Alexander; Pigneur, Yves et al: Business Model Generation, campus Verlag, 2013 (and more recent editions)
Ries, Eric: Lean Startup, 4th ed. Reline-Verlag Munich 2015
Kotsemir, M.; Abroskin, A.; Meissner, D.: Innovation Concepts and Typology - an evolutionary
Discussion. Basic Research Programme, Working papers, SERIES: SCIENCE, TECHNOLOGY AND INNOVATION WP BRP 05/STI/2013

Supplementary:
Christensen, Clayton M.: The Innovators Dilemma, Harvard Business Review Press (1997 and current editions, also available in German)
Burkhardt, Christoph: Thinking error innovation; SpringerGabler 2017

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5100240,6810210
Programming Project

Module profile

Exam number
5100240,6810210

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 12 hrs

Self-study: 138 hrs

Total: 150 hrs

Teaching format
Seminar

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun

Applicability	BISD, BIN
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
BIN: Programming I and Programming II
BISD: Programming I

Recommended prerequisites for the participation in the module
Programming I + II
Databases I
Software Engineering I

Content
The students should realise their own application in groups. An application could, for example, be a game, a three-tier web application or a comparable application. Possible parts of the application could be a graphical user interface (including a web interface), database connection including schema design, network communication, AI, etc. The students also create documentation (general overview, various use cases, the most important activity and sequence diagrams, etc.).

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
After successfully completing the module, students will be able to

- develop a first larger application in a team of 4-6 people
- carry out and implement project planning
- carry out and implement a task distribution
- apply their knowledge of software design
- apply programming concepts they have learnt
- look up required content themselves using suitable literature
- break down a task into sub-problems.

Literature
None

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810220
Computer Architecture

Module profile

Exam number
6810220

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction, Exercise

Language of instruction
German

Organisation

Responsible lecturer
Prof. Dr. Christian Bachmeir

Lecturer(s)
Prof. Dr. Christian Bachmeir

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
Fundamentals of Computer Engineering

Content
- Historical development
- Calculator classifications (Flynn, Händler, Giloi)
- Computer arithmetic (representation of characters and numbers, IEEE 745, basic arithmetic operations, Booth algorithm)
- Microcomputer core with control and arithmetic unit (pipeline concept, dependencies and their resolution, dynamic scheduling: scoreboard, Tomasulo)
- Machine instructions (ISA, addressing types, assembler programming)
- x86 assembler (nasm, Linux/Ubuntu)
- RISC / CISC concepts (resource conflicts, µprogramming)
- Memory (structure of DRAM, SRAM, caches, coherence protocols)
- I/O and peripherals (external memory, buses)
- Parallel computers and multithreading
- Performance evaluation (basic terms, benchmarks)

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Written exam (sP) according to § 23 APO

Examination - length/format
90 minutes

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German

Condition for the award of credit points
None

Learning outcomes
Students gain an understanding of the structure and operation of computer systems,
and the operation of different computer architectures.
They also acquire basic knowledge in the field of embedded systems.
.
Students are able to

- visualise basic components of simple computers,
- explain different forms of realisation of complex circuits,
- describe relevant memory technologies,
- analyse the structure and programming of processors,
- implement simple assembler programmes and take into account specific characteristics of a computer when programming,
- evaluate the performance of computers,
- design subcomponents of a simple computer.

Literature
J. Hennessy, D. Patterson: Computer Architecture, A Quantitative Approach, 2017
J. Hennessy, D. Patterson: Computer Organisation and Design, 2022
U. Brinkschulte, T. Ungerer: Microcontrollers and Microprocessors, 2002
A. Tanenbaum: Structured Computer Organisation, 2021
W. Coy: Structure and operation of computer systems, 1992
P. Hermann: Computer architecture, 2013
H. Bähring: Microcomputer systems, 1994
C. Märtin: Introduction to computer architectures, 2003
H. Malz: Computer Architecture, 2004
W. Oberschelp, G. Vossen: Rechneraufbau und Rechnerstrukturen, 2006
B. Bundschuh, P. Sokolowsky: Computer Structures and Computer Architectures, 1996
Todd Austin Andrew S. Tanenbaum. Computer Architecture: From Digital Logic to Parallel Computing. Pearson, 2014
John L. Hennessy David A. Patterson. Computer Organisation and Design: The Hardware/Software Interface. Morgan Kaufmann Publishers, 1994
Matthias Homeister. Understanding Quantum Computing: Fundamentals-Applications-Perspectives. Springer-Verlag, 2022
Vossen Oberschelp. Computer Architecture. Oldenbourg-Verlag, 2006
Fundamentals of Computer Architecture, Frank Slomka, Michael Glaß, Springer, 2023
Basic course in computer science, Ernst, Schmidt, Beneken, Springer, 2023

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810230
Security Operations

Module profile

Exam number
6810230

Duration
1 semester

Frequency
Every summer semester

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
German/English

Organisation

Responsible lecturer
Prof. Dr.-Ing. Tobias Fertig

Lecturer(s)
Prof. Dr.-Ing. Tobias Fertig, Dr.-Ing. Rodrigo Daniel do Carmo

Applicability	BISD
Semester according to SPO	4. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
none

Recommended prerequisites for the participation in the module
none

Content
Students learn how to secure networks and IT systems using technical protective measures. The focus is on central security components such as firewalls, proxies and intrusion detection systems (IDS). Students acquire practical knowledge of how to set up, configure and use these systems in realistic scenarios. The content is based on the typical requirements of a corporate environment and established security standards such as those of the National Institute of Standards and Technology (NIST). A special focus is placed on the topic of security monitoring: students learn to identify, correlate and analyse security-relevant information from various sources in a targeted manner. They develop and implement case-specific detection rules for attack detection and deal with the tasks and processes of a Security Operations Centre (SOC), including logging, incident detection and response. The module thus provides a practical understanding of the operation of IT security systems in modern corporate environments.

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Practical study achievement

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes

- Students know the functions of firewalls, proxies and intrusion detection systems and can set them up
- Students can develop and implement case-specific rules for recognising attacks
- Students can identify and collate security-relevant information for security monitoring
- Students know the tasks of a Security Operations Centre (SOC)

Literature

Defensive Security Handbook: Best Practices for Securing Infrastructure, Lee Brotherston and Amanda Berlin, 2017
Zero Trust Security: An Enterprise Guide, Jason Garbis and Jerry W. Chapman, 2021
Security Operations Centre: Building, Operating and Maintaining Your SOC, Joseph Muniz and Gary McIntyre, 2015

5. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 6810250
Supervised Internship

Module profile

Exam number
6810250

Duration
1 semester

Frequency
Every semester

Credit hours (SWS)
1

ECTS-Credits (CP)
30.0

Workload
Guided study time:
Presence time: 15 hrs

Self-study: 885 hrs

Total: 900 hrs

Teaching format
Practice

Language of instruction
German/English

Organisation

Responsible lecturer
Michael Rott

Lecturer(s)
Michael Rott

Applicability	BISD
Semester according to SPO	5. semester
Type of module	Compulsory module

Required prerequisites for the participation in the module according to the SPO
> 90 ECTS points. 55 ECTS from 1st year

Recommended prerequisites for the participation in the module
none

Content

- As part of a larger IT project, you will be required to work independently in as many project phases as possible (system analysis, system planning, implementation, system introduction and testing). This project should last at least 12 weeks.
- Ideally, the intern will familiarise themselves with various departments and areas of the company prior to the project in order to gain a rough understanding of other departments and the company as a whole.

The contact person/supervisor at the FHWS is the representative for the supervised practical phase, Prof. Dr Tobias Aubele

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Documentation, Presentation

The concrete length/format of the examination will be determined in the study plan.

Language of examination
German/English

Condition for the award of credit points
None

Learning outcomes
The trainee should

- acquire relevant, practice-orientated knowledge of operational processes
- learn (through guidance) to work independently and autonomously in IT projects.
- combine competences acquired during their studies with practical experience.
- learn to understand problems and requirements (e.g. customer requirements).
- learn to design and implement solutions to problems (e.g. for company processes and/or IT projects).
- experience working in a team.
- get to know and experience embedding in the company, its processes and organisational procedures.
- get to know and experience the IT profession.
- learn to approach the right people when problems arise.
- learn about the unconditional will to successfully and professionally realise projects.
- experience excellence and professionalism.
- experience how employees are captivated.
- recognise and feel the meaning of their work.

Literature
No general literature recommendation possible

7. semester

fiw.thws
Faculty of Computer Science and Business Information Systems
Technical University of Applied Sciences Würzburg-Schweinfurt

Module: 5003198
Green IT (Blended Intensive Program)

Module profile

Exam number
5003198

Duration
1 semester

Frequency
Irregular

Credit hours (SWS)
4

ECTS-Credits (CP)
5.0

Workload
Guided study time:
Presence time: 60 hrs

Self-study: 90 hrs

Total: 150 hrs

Teaching format
Seminar-style instruction

Language of instruction
English

Organisation

Responsible lecturer
Prof. Dr. Peter Braun

Lecturer(s)
Prof. Dr. Peter Braun,
Prof. Dr. Frank-Michael Schleif

Applicability	BIN, BWI, BEC, BISD, BDGD
Semester according to SPO	7. semester
Type of module	FWPM

Required prerequisites for the participation in the module according to the SPO
None

Recommended prerequisites for the participation in the module
None

Content
This module explores how sustainability principles can be integrated into the design, development, deployment, and management of IT systems. It offers a multidisciplinary perspective on the environmental, economic, and societal implications of information technology. Through lectures, case studies, and collaborative international projects, students gain both theoretical foundations and practical experience in Green IT strategies. Partnering with universities in the Czech Republic, Germany, and Iceland, the module includes cross-border collaboration and comparative analysis of regional IT sustainability approaches. This module contains a compulsory study trip to Prague, the Czech Republic.

- Introduction to Green IT: Definition, significance, and global relevance; real-world applications in industry and academia
- Environmental Impact of IT: Carbon footprint, e-waste, lifecycle analysis, and Green Computing standards
- Sustainable Software Engineering: Design principles and code optimisation for energy efficiency
- Green Algorithms and Data Structures: Techniques to reduce energy consumption and benchmark software for efficiency
- AI and Machine Learning for Green IT: Optimisation of energy use, environmental monitoring, and ethical implications
- Green IT Strategies in Mobile and Distributed Systems: Sustainable design and management of mobile technologies and data centres
- Life Cycle Assessment (LCA): Application of LCA in IT hardware and software development
- Education and Training for Green IT: Curriculum development, capacity building, and case studies
- Regulatory and Compliance Aspects: Overview of international standards, compliance practices, and green certifications

Examination

Required prerequisites for the participation in the examination according to the SPO appendix
None

Examination - type
Other exam (soP) according to §§ 26, 27 APO

Examination - length/format
Portfolio

The concrete length/format of the examination will be determined in the study plan.

Language of examination
English

Condition for the award of credit points
None

Learning outcomes
Upon successful completion of this module, students will be able to:

- Remember key concepts and terminology related to Green IT, including sustainability goals, environmental impacts, and regulatory frameworks
- Understand the ecological footprint of hardware and software systems and explain how IT contributes to global sustainability challenges
- Apply principles of sustainable software engineering, energy-efficient algorithms, and lifecycle assessments to practical use cases
- Analyse and compare national and regional Green IT strategies and regulatory approaches across Germany, Iceland, and the Czech Republic
- Evaluate the sustainability impact of IT systems and development practices using recognised metrics and standards
- Create innovative, practical solutions to real-world Green IT challenges by working on interdisciplinary, cross-national projects

Literature
It will be announced in class