University of Applied Sciences St. Pölten

Computing Module

Summer Semester 2026

Language of instruction: English

Last update: 24 September 2025

Hochschule für Angewandte Wissenschaften St. Pölten GmbH, Campus-Platz 1, 3100 St. Pölten, +43 2742 313 228-200, csc@ustp.at, ustp.at
Firmenbuch LG St. Pölten, FN 146616m, UID ATU 53208201

EUDRES

Please find a list of all eligible courses below. Course descriptions can be found on our MCR[1], MIR[2] and EFH[3] websites. Please note that the list might be subject to alterations.

Subject Code	Study Programme	Semester	Subject	ECTS credits
27742	MIR	2	IT Governance	5
25937	MIR	2	Innovation Management and Product Development	5
29325	MIR	2	Publishing and Presentation	5
tba	MIR	2	Elective: Foundations of Symbolic AI** **or** Elective: Introduction to Spatial Data Analysis**	5
21814 21815	MCR	2	Digital Forensics and Incident Handling* **+** Professional Report Writing*	4 **+** 1
21823	MCR	2	Threat Modeling & Information Sharing	5
21816	MCR	2	Application Security and Pentesting	5
21817 21818	MCR	2	Security Auditing* **+** Audit Interview Skills*	4 **+** 1

25303	MCR	2	Leadership	3
25302	MCR	2	Complex Problem Solving	2
21835	MCR	4	Master Thesis & Diploma Seminar	23
tba	EFH-1	2	German 1 **or** German 2	3 3
tba	EFH-1	2	Scouting Austrian Culture	3

* Please note that these two subjects can only be taken together

** Please note that these subjects take place at the same time, therefore you can **only take one** of those subjects

MCR = Master Cyber Security and Resilience. For further information and course descriptions, please visit: https://www.ustp.at/de/studium-weiterbildung/informatik-security/cyber-security-and-resilience/studieninhalte#/

MIR = Digital Innovation and Research. For further information and course descriptions, please visit: https://www.ustp.at/en/academic-studies-continuing-education/computer-science-security/digital-innovation-and-research/course-contents?set_language=en#/

EFH = Courses in German language and Austrian culture. For further information and course descriptions, please visit: https://www.ustp.at/en/international/incoming-students/german-language-classes

Teaching days for German Language: Tuesdays in the afternoon/evening
Teaching days für Austrian Culture: blocked workshop sessions on Saturdays

All study programmes at the Department of Computer Science and Security teach in a blocked system. There is always one course at a time for 2-3 weeks and then the next course will start (e.g., 3 weeks Artificial Intelligence then two weeks Design Thinking). Classes are usually held from 8:50 to 15:30 with a lunch break. Every study programme has fixed teaching days:

MIR: Monday and Tuesday (exception: Elective)

MCR: Wednesday, Thursday and Friday

Please see all course descriptions below.

IT Governance (MIR)

Learning outcomes

- Students can explain important legal terms
- Students are able to discuss relevant data protection regulations (e.g. DSG2000, GDPR, etc.) and can apply key aspects to problems.
- Students are able to determine legal data protection requirements with regard to data collection, storage and processing from laws
- Students can explain IT Governance related Standards
- Students can identify and implement legal requirements for the protection of intellectual property
- Students are able to explain and apply the terns and concepts of data governance.
- Students know the concept of agile Data Governance
- Students know relevant sources of data, important data formats and can apply methods to evaluate the data quality.
- Students are able to formulate organizational and technical requirements of data security.

Course Content

- Exploitation of rights in the national and international environment
- Trade in rights, patents and licenses with special attention to digital rights management and dual licensing, open source, open data, open innovation
- Privacy and information, GDPR
- IT Standards and Guidelines
- Data Governance / Managements / Data Curation
- Definition of entity and identity
- Management of databases and data access
- Meta data, Data archives and storage
- Data Mesh vs Data Warehouse vs Data Lake Security

- Internal control mechanisms / control systems
- Organizational foundations of data protection
- Risk assessment
- Norms, standards and best practices (ISO29xxx, ISO270xx, standard data protection methods,…)

Innovation Management and Product Development (MIR)

Learning outcomes

After completing the course, students can

- understand the challenge of an innovation process
- understand the connection between invention, innovation and product development
- understand the advantages and disadvantages of simultaneous engineering
- transfer the methods of innovation management and product development to a concrete practical or theoretical question in practice

Course Content

An invention is a creative achievement as a result of research and development, the first technical realisation of a new problem solution. Innovation is the economic application of a new solution to a problem, i.e. it leads to an economic optimisation of the exploitation of knowledge. In the context of the innovation process and product development, many boundary conditions have to be considered and product and process questions have to be examined.

The challenges of an innovation process and the connections between invention, innovation and product development are the contents of this course.

Publishing and Presentation (MIR)

Learning outcomes

- Students are able to describe the characteristics of scientific papers, project proposals and reports and to make use of these text forms for their own work.
- The students can (under guidance) write a scientific article for an international scientific journal. The aim is for the students to develop a scientific article ready for publication and to submit it to a conference or a journal.
- Students learn the presentation of scientific results in English in an understandable manner and their oral presentation.
- Students can describe the course of a conference session (lecture, discussion, moderation)
- On the basis of original papers, students are able to write an elaboration (lecture and poster) on a topic chosen in consultation with the responsible lecturers.
- Students can present a defined topic according to the guidelines they have learned.

Course Content

- Text comprehension (technical texts)
- Explanation and description of technical processes
- Short presentations, Case studies
- Expansion of vocabulary, especially in the field of technology
- Improvement of writing and speaking skills through working on selected technical texts and through suitable simulations of specific situations
- Journals & conferences and selection of journals and conferences
- Structure of a work
- Literature research and administration.
- Journal from publisher's side and Peer Review

Elective (MIR)

Option 1: Foundations of Symbolic AI - Teaching Days: Thursday & Friday

The offered course covers important theoretical aspects of computer science and artificial intelligence.

Important topics include (but are not limited to):

- Basic concepts of semiotics
- Basic concepts of complexity theory
- Introduction to formal languages
- Turing Tests, intelligent machines,…

Option 2: Introduction to Spatial Data Analysis - Teaching Days: Thursday & Friday

The course offered covers important aspects of the use of geographical data and geo information systems.

Important topics include (but are not limited to):

- Spatial market segmentation
- Routing and point patterns
- Geostatistics

Digital Forensics and Incident Handling (MCR)

Learning outcomes

- Students will be familiar with the basic principles of IT forensics and incident handling
- The students have the knowledge to assess security-critical cases and to be able to take initial measures or carry out analyses
- They have knowledge of the structure and analysis of different file systems and can explain their properties and special features.
- The students know common forensic and incident handling tools and can use them
- Students can autonomously carry out acquisition and post-mortem analysis of information technology systems (hard disk, RAM) as well as mobile devices (Android, iOS) and combine them into a forensically sound analysis.
- Students can prepare a forensic report taking into account formal criteria and observing the basic principles of digital forensics, analyse and question results, and present them in a target group-oriented manner.

Course Content

Overview of practices and procedures in digital forensics and incident handling

- integrity
- chain of custody
- order of volatility
- Forensic process
o Identification
o Digital preservation of evidence (acquisition)
o Analysis
o Reporting
- profiling

Standards:

- ISO/IEC 27037:2012

- ISO/IEC 27041:2015
- ISO/IEC 27042:2015
- ISO/IEC 27043:2015
- ISO/IEC 27050:2016+

Incident response and digital forensics with focus on company processes

Incident handling process (preparation, identification, containment, remediation, recovery)

Log Analysis for Incident Responders

file system forensics

- NTFS
- Ext
- iOS
- android

live forensics

- Monitoring tools for recording file system activity
- Tracing tools for API or Native/System calls
- Integration of network traffic into the forensic process

Application forensics (databases of concrete applications), e.g:

- browser data
- User communication (instant messaging, e-mail)

Professional Report Writing (MCR)

Learning outcomes

- Students are able to structure reports.
- Students can write reports for specific target groups.

Course Content

- Target group analysis
- Types of reports
- Structuring of reports
- Joint preparation of reports
- Targeted writing (e.g.: forensic expert opinion for court)

Threat Modeling and Information Sharing (MCR)

Learning outcomes

- The students understand how models are basically structured and can develop and abstract examples
- The students know the central aspects of threat modelling and can read, interpret and question given threat models from the field of attack defense and vulnerability modelling
- Students can individually apply threat modelling techniques to the risk analysis process and develop new threat scenarios in fictitious organisations
- The students are able to transfer reports, (technical) indicators and data sets into common threat models and visualize them
- The students know the possibilities and tools of strategic, tactical and operational threat intelligence and are able to apply them
- The students are able to independently extract indicators of compromise from information resources and to transfer them automatically and also manually into common formats (e.g. STIX)

Course Content

Threat modeling

- Fundamentals of Modeling
o Properties of models
o Information theory (syntax, semantics, pragmatics)
o Abstraction
- Aspects of threat modeling
o Actors and motivation
o Tactics, Techniques and Procedures (TTPs)
o Observables or compromise indicators (IoCs)
- Common threat modeling techniques and models, including
o Attack Trees and Attack-Defense Trees
o STRIDE and PASTA
o Kill Chains
- Attack Patterns and Vulnerabilities
o Mapping of attack techniques and attack phases in the environment of IT systems (CAPEC, ATT&CK, etc.)
o Modeling and quantification of software weak points and vulnerabilities (CVSS, CWE)
- Visualization and creative techniques, among others:
o Persona non Grata
o Security Cards
o Gamification and Serious Games
- Integrated threat modeling
o Interfaces to organizational processes
o Interaction with the operational risk analysis

Exchange of information at organisational and technical level
- Threat Intelligence: Collection, Evaluation, Analysis, Structuring
o Strategic (trends and risks)
o Tactical (Indicators of Compromise)
o Operational (technical approaches)
- Vocabularies and Formats

o STIX, TAXII, CybOX
- In-house preparation and communication
- Inter-organizational exchange of threat information
- Computer Emergency Response Teams (CERTs)

Application Security and Pentesting (MCR)

Learning outcomes

- Students understand the different stages of a professional hacking attack (e.g. Cyber Kill Chain).
- Students can build a professional hacking lab environment to practically test and practice attacks.
- Students can use relevant pentesting tools such as Nmap, Wireshark, Metasploit ....
- Students understand how exploits are executed to compromise Windows and Linux systems and gain access.
- Students understand the procedures and techniques used by hackers to attack web servers and web applications such as SQL injection, cross site scripting, etc. and can apply them themselves.
- The students can use the methods and tools to test WLAN and mobile systems for their security.
- Students can evaluate risks of found vulnerabilities.

Course Content

- Basics of application security and penetration testing
- Establishment of a suitable hacking lab
- Procedures of a professional penetration tester
- Frameworks, tools and methods for penetration testing
- OWASP Top 10 / OWASP Testing Guides

Security Auditing (MCR)

Learning outcomes

- The students know basic terms (e.g. audit universe, control) and can explain them.
- Students can plan audit programs and audits .
- Students are able to independently develop audit guidelines based on predefined standards.

Course Content

Tasks and function of an auditor

Internal control systems (structure, ...)

Audit process:

- Defining the audit objectives and scope
- audit planning
- audit execution
- reporting

Important standards and good practices

Audit Interview Skills (MCR)

Learning outcomes

- Students can carry out audit interviews and document findings in a comprehensible manner
- The students are able to present their results and summarize them in a report

Course Content

- Basics of question technique.
- Conducting audit interviews.

Leadership (MCR)

Learning outcomes

- Students understand management tasks in an organization
- The students know frequent challenges and problems in the area of leadership
- Students can identify / analyse different leadership styles and know their own leadership style

Course Content

- Basics of leadership
- Management styles
- Conflict management
- Communication & Conversation with employees
- Basics of strategic management (vision, analysis of weaknesses and strengths of anorganization/team)
- Self-reflection

Complex Problem Solving (MCR)

Learning outcomes

- Students are able to analyse problems
- Students can use different methods to find causes and analyse problems
- Students are able to find solutions to identified problems.

Course Content

- Strategic Thinking
  - Frame the problem
  - Diagnose the problem
  - Find solutions
  - Implement solution
- Root Cause Analysis Techniques.