



Valid from 2025.HS

Module description: Cyber Security and Data Protection	
Module Code	t.BA.MI.CSDS.23HS
ECTS Credits	4
Language of Instruction/Examination	German
Organizational Unit	InIT
Module Coordinator	Mirjam Blumenstein
Legal Framework	The module description is part of the legal basis in addition to the general academic regulations. It is binding. During the first week of the semester a written and communicated supplement can specify the module description in more detail.
Module Characteristic	Type 2a 4 consecutive lecture lessons per semester week and class
Module Description	This module provides students with fundamental knowledge in the areas of cyber security and data protection, particularly in the context of medical informatics. Students learn how to protect systems and data from attack and misuse, and how to develop and apply data protection policies and procedures.
Module Content	This course introduces fundamental aspects of information security and data protection, with a special focus and examples from the healthcare sector. The theoretical lectures are complemented by practical exercises. The following topics are covered in this lecture: Introduction, Cyber Security Frameworks Privacy Cryptography Access control Network security Incidentmanagement Application security Medical Device Security Security Awareness
Prerequisite Knowledge	

Module description: Cyber Security and Data Protection

Learning Objectives (Competences)	Students...		Competencies	Taxonomies		
	Participants will develop a foundational understanding of information security principles, including confidentiality, integrity, and availability of data, as well as relevant threats and protective measures.		F, M	K1, K2, K3		
	Participants will learn to systematically analyze and assess risks, as well as develop and implement effective risk mitigation strategies.		F	K2, K4, K5		
	Participants will understand how technical, organizational, and physical security controls work together to create a comprehensive security strategy.		F, M	K2, K3		
	Participants will learn the fundamental principles of data protection, including legal and regulatory requirements (e.g., GDPR, Swiss DSG). They will be able to implement appropriate measures to ensure secure processing of personal data and apply data protection policies within an organizational context.		F	K2, K3, K4		
	Participants will learn to handle security incidents in a structured manner—from detection and response to recovery. Additionally, they will understand the importance of continuous monitoring to identify and mitigate potential threats at an early stage.		F, M	K2, K3, K4		
Performance Assessment	End-of-module exam		Assessment	Length (min.)	Weighting	Form
	written exam			90	90	acc. to module agreement
	Performance assessment during the semester		Assessment	Length (min.)	Weighting	Form
	Labs <i>Labs</i>		predicate		10	acc. to module agreement
Classroom Attendance Requirement	None					
Learning material	<ul style="list-style-type: none"> Sean P. Murphy, Healthcare Information Security and Privacy, 2015 William Stallings, Computer Security, 4th Edition, Pearson, 2017 					
Comments						