Subject	**Technology and Security**			
	Type	**Semester**	**ECTS**	**Code**
	MANDATORY (O)	2	4	
Course Lecturer				
Aims and Objectives	The course will include the historical background of security, the fundamentals of information systems security, privacy and the importance of security for information systems. Additional topics include protection schemes, Global cybersecurity threatens, cybersecurity Behaviours, malicious security threats (viruses, worms, Trojan horses) and online security.			

Learning Outcomes	Upon completion of this course: • Students will be able to define concepts of confidentiality, availability, and integrity as they relate to information security. • Students will understand the potential threats of information systems • Students will be able to define the concepts of authentication, non- evaluation, access control and privacy • Understand information security theories and principles • Defence mechanisms understand both their strengths and limitations
	• Demonstrate how to ensure the use of files and users

Course Content	**Course Plan**	**Week**
	Technology Changing and Digital Transformation security	1
	What is information Security	2
	Information security goals	3
	Data Analytics / Importance of Accessing Data	4
	Risk Management Threats and Vulnerabilities	5
	Types of attacks / National Cyber Attacks	6
	Cybersecurity Behaviours	7
	Information security policies, guidelines and procedures.	8
	Global Cyber Threatens	9
	National Cybersecurity Ecosystem	10
	Critical Security Infrastructure	11
	Cybersecurity Gamification	12
	Presentations of research papers	13
	Presentations of research papers	14
	Course summary: Reflection &Review	15

Teaching/Learning Assessment Methods	**Teaching/Learning Activity**	**Weight (%)**
	1. Lectures	60%
	2. Term Project	20%
	3. Case studies	10%
	4. Laboratory	10%

Assessment Activity	**Number**	**Week**	**Weight (%)**
1. Attendance	12	1-12	5%
2. Seminar Paper*	1	9	25%
3. Final Exam			70%

* The seminar paper is mandatory and conditions for the final. exam.

Course resources	**Resources**	**Number**
	1. Class	1
	2. Laboratory	1
	3. Moodle	1
	4. Projector	1

ECTS Workload	**Activity**	**Weekly**	**Total workload**
	1. Lectures	2	30
	2. Seminars	1	15

	3.Laboratory		10
	4. Independent learning	12	40
	6. Exam/presentations		5

Literature/References	**Text Book** 1. Principles of Information Security (MindTap Course List) 7th Edition by Michael E. Whitman (Author), Herbert J. Mattord 2. Fundamentals of Information Systems Security 4th Edition by David Kim (Author), Michael G. Solomon 3. Infosec Strategies and Best Practices: Gain proficiency in information security using expert-level strategies and best practices by Joseph MacMillan 4. Hackable: How to Do Application Security Right by Ted Harrington 5. Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects by Ed Moyle (Author), Diana Kelley **Reference Book** 1. Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects by Ed Moyle (Author), Diana Kelley 2. Privilege Escalation Techniques: Learn the art of exploiting Windows and Linux systems by Alexis Ahmed 3. Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition by Ross Anderson 4. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff 5. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World Joseph Menn •
Contact	