SYLLABUS

1. Data about the program of study

1.1 Institution	The Technical University of Cluj-Napoca
1.2 Faculty	Faculty of Automation and Computer Science
1.3 Department	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Information Security***			Subject code	**2.00**
2.2 Course responsible / lecturer	Lect. dr. eng. Marius Joldoș - Marius.Joldos@cs.utcluj.ro				
2.3 Teachers in charge of seminars / Laboratory / project	Lect. dr. eng. Marius Joldoș - Marius.Joldos@cs.utcluj.ro				
2.4 Year of study		2.5 Semester		2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DS
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DI

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminars	1	Laboratory	-	Project	-
3.2 Number of hours per semester	42	of which:	Course	28	Seminars	14	Laboratory	-	Project	-
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										50
(b) Supplementary study in the library, online and in the field										20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										11
(d) Tutoring										-
(e) Exams and tests										2
(f) Other activities:										-

3.4 Total hours of individual study (sum of (3.3(a)…3.3(f)))	83
3.5 Total hours per semester (3.2+3.4)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	-
4.2 Competence	Operating systems architecture, computer architecture, basic computer networks knowledge

5. Requirements (where appropriate)

5.1. For the course	Video projector, MS Teams Platform, Moodle Platform
5.2. For the applications	Video projector, MS Teams Platform, Moodle Platform. Seminar attendance is mandatory

6. Specific competence

6.1 Professional competences	Secure sensitive customer's information Develop information security strategy Provide ICT consulting advice Manage IT security compliances Manage data for legal matters Identify ICT system weaknesses Identify ICT security risks Educate on data confidentiality Ensure adherence to organizational ICT standards Communicate with stakeholders Manage system security Implement ICT risk management Advice on security risk management Establish an Information Security Management System
6.2 Cross competences	Develop an analytical approach Taking a proactive approach Developing strategies to solve problems Being open minded Work in teams

7. Expected Learning Outcomes

Knowledge	Explain fundamental information security concepts, including confidentiality, integrity, availability (the CIA triad), non-repudiation, and authentication. Identify and categorize different types of threats, vulnerabilities, and attacks that target computer systems and networks. This includes understanding the motivations behind various cyber attacks. Analyze the ethical, legal, and social implications of cybersecurity practices, and understand the responsibilities of a cybersecurity professional.
Skills	Assess and analyze security risks using established frameworks and methodologies, and develop a basic risk management plan. Evaluate the security posture of a given system or network, and recommend appropriate security measures to mitigate identified risks. Communicate effectively on technical and non-technical aspects of information security, both in writing and verbally. This includes being able to explain complex security concepts to a non-technical audience.
Responsibilities and autonomy	Collaborate effectively in teams to address security challenges and solve problems, reflecting the collaborative nature of the cybersecurity field. Demonstrate a professional and ethical approach to handling sensitive information and security incidents, adhering to legal and regulatory requirements. Take initiative in a professional context by independently researching and staying current with emerging threats, vulnerabilities, and security technologies. Manage and organize their own work effectively and reflect on their learning and the progress of their knowledge and skills in the field.

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	Acquiring a global, comprehensive view on the many areas and aspects which are part or are directly connected with computer systems, networks, and information security. Understanding the applicability of notions and information security specific elements to the real world (and, particularly to software and computer systems) and acquiring an ability to observe, analyze and evaluate the connections of information security with the real world.
8.2 Specific objectives	Familiarization with information security specific terminology and correct use of that terminology. Understanding the various aspects and ways that connect cybercrime and information security to day-to-day activities. Acquiring an ability to analyze an information system from the point of view of information security (for example, a critical viewpoint). Acquiring an overall view and the ability to connect the various engineering

	areas, various software project types, the field, and the elements specific to information security and the applicable standards and procedures. Familiarization with the fundamental domains (as stated in CISSP) of information security.

9. Contents

8.1 Lectures	Hours	Teaching methods	Notes
Introduction and context. Cyber-crime impact on society. Cyber-attacks & malware	2	Blackboard illustrations and explanations, beamer presentations, discussions, short challenges	Uses a video-projector
Cybersecurity ethics	2		
Access control	2		
Risk management (I)	2		
Risk management (II)	2		
Security systems architecture and design (I)	2		
Security systems architecture and design (II)	2		
Physical and environmental security	2		
Laws, regulations, investigations and compliance (I)	2		
Laws, regulations, investigations and compliance (II)	2		
Operations security (I)	2		
Operations security (II)	2		
Software Development Security (I)	2		
Software Development Security (II)	2		
Bibliography: 1. CISSP Exam Guide – Maymi, F. and Harris, S. – McGraw-Hill, 2022, 9th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2017, 3nd edition 3. Geekonomics. The Real Cost of Insecure Software – Rice, D. – Addison-Wesley, 2008 4. Various articles and technical reports from the specialists of the field – in electronic format.			
8.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Economic and social impact of cybercrime	2	Student presentations, discussions, case studies	
Social engineering and Trust	2		
Analysis of recent technical reports and articles (1)	2		
Analysis of recent technical reports and articles (2)	2		
Analysis of recent technical reports and articles (3)	2		
Analysis of recent technical reports and articles (4)	2		
Analysis of recent technical reports and articles (5)	2		
Bibliography: 1. Harris, S. & Maymi, F. – CISSP Exam Guide – McGraw-Hill, 2022, Ed. 9 2. Vacca, J. – Computer and Information Security Handbook – Morgan Kaufmann, 2017, Ed. 3 3. Moodle course Web Site available at https://moodle.cs.utcluj.ro/			

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

The fundaments of this course rely on the CISSP® (Certified Information Systems Security Professional), one of the most important certifications in information security, internationally appreciated and recognized (https://www.isc2.org/cissp/default.aspx). There are periodical discussions with the representatives of significant employers, especially the ones that develop projects in information security.

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Ability to solve domain-specific problems. Activity, interaction during the lectures	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of different subjects / paper in the course's field during the semester. In exceptional cases, which demand remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	80%
Seminar	Ability to solve domain-specific problems. Activity, interaction during the lectures	Presentation of a research result and/or presentation of a solution similar to the one discussed at the seminar. In exceptional cases, which imposes remote classes, the exam could be given online remotely, using Moodle and Teams platforms.	20%

Minimum standard of performance:
Attending minimum 50% of lecture classes, to be allowed to take the final examination. Attending all lab classes (one lab could be recovered during the semester, and one more during re-examination sessions).
Evaluation grade ≥ 5 (out of 10).
Demonstration of understanding of the concepts and notions of information security, and their correct use and application. The ability to critically analyze of a case study and the ability to define and explain the specific terms used.

Date of filling in: 01.09.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Lect. dr. eng. Marius Joldoș	
	Applications	Lect. dr. eng. Marius Joldoș	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureșan