COURSE SYLLABUS

Academic year 2025 - 2026

1. Programme Information

1.1. Higher education institution	Lucian Blaga University of Sibiu
1.2. Faculty	Faculty of Science
1.3. Department	Mathematics and Informatics
1.4. Field of study	Informatics
1.5. Level of study[1]	Master
1.6. Programme of study/qualification	Cybersecurity

2. Course Information

2.1. Name of course	Security and privacy					Code	FSTI.MAI.CS.M.SA.3.2020.E-7.2
2.2. Course coordinator	Professor PhD. Ana-Maria Acu						
2.3. Seminar/laboratory coordinator	Professor PhD. Ana-Maria Acu						
2.4. Year of study[2]	2	2.5. Semester[3]	1	2.6. Evaluation form[4]	E		
2.7. Course type[5]	O	2.8. The formative category of the course[6]	S				

3. Estimated Total Time

3.1. Course Extension within the Curriculum – Number of Hours per Week				
3.1.a. Lecture	3.1.b. Seminar	3.1.c. Laboratory	3.1.d. Project	Total
2		2		**4**
3.2. Course Extension within the Curriculum – Total Number of Hours within the Curriculum				
3.2.a. Lecture	3.2.b. Seminar	3.2.c. Laboratory	3.2.d. Project	Total[7]
28		28		**56**

Time Distribution for Individual Study[8]	**Hours**
Learning by using course materials, references and personal notes	38
Additional learning by using library facilities, electronic databases and on-site information	37
Preparing seminars / laboratories, homework, portfolios and essays	28
Tutorial activities[9]	14
Exams[10]	2
3.3. Total Individual Study Hours[11] *($NOSI_{sem}$)*	**119**
3.4. Total Hours in the Curriculum *($NOAD_{sem}$)*	**56**
3.5. Total Hours per Semester[12] *($NOAD_{sem} + NOSI_{sem}$)*	**175**
3.6. No. of Hours / ECTS	**25**
3.7. Number of credits[13]	**7**

4. Prerequisites (if needed)

4.1. Courses that must be successfully completed first (from the curriculum)[14]	-
4.2. Competencies	-

5. Conditions (where applicable)

5.1. For course/lectures[15]	Classroom, equipped with blackboard, computer, video projector and software
5.2. For practical activities (lab/sem/pr/app) [16]	Laboratory room equipped with computers

6. Learning Outcomes [17]

Number of credits assigned to the discipline: 7				
Learning outcomes				Credit distribution by learning outcomes
Nr. crt.	Knowledge	Skills	Responsibility and autonomy	
LO 1	The student explains the fundamental concepts of security and privacy, including cryptographic basics and secure communication protocols.	The student applies encryption methods, digital signatures, and communication security protocols.	The student demonstrates responsibility in selecting protection mechanisms and complies with legal and ethical standards.	1.5
LO 2	The student describes security measures for networks, operating systems, and web applications.	The student configures firewalls, IDS/IPS, VPNs, and applies protection techniques in Windows, Linux, and web applications.	The student assumes responsibility for protecting resources and adopts professional best practices.	2
LO 3	The student understands security issues related to mobile devices and cloud infrastructures.	The student implements security solutions for mobile applications, devices, and cloud environments (encryption, access management, MDM).	The student shows autonomy in using emerging technologies and complies with data protection regulations.	1.5
LO 4	The student explains the role of privacy legislation and technologies.	The student applies privacy best practices and uses anonymization and differential privacy technologies.	The student demonstrates high responsibility in protecting personal data and adopts ethical conduct.	1
LO 5	The student describes incident response procedures, digital forensics elements, as well as ethical hacking and security management principles.	The student applies incident response procedures, performs penetration testing, and uses audit and compliance tools.	The student assumes responsibility for the accuracy of assessments and complies with legal and governance frameworks.	1

7. Course objectives (resulted from developed competencies)

7.1. Main course objective	The main objective for security and privacy is to staying current with new threats, regulations, and best practices in security and privacy management.
7.2. Specific course objectives	Specific objectives for security and privacy are: confidentiality, integrity, availability, privacy, compliance, risk management, continuous improvement

8. Content

8.1. Lectures[18]	**Teaching methods**[19]	**Hours**
Introduction to Security and Privacy: an overview of the key concepts and principles of security and privacy.	Lecture, use of video projector, discussions with students	2
Cryptography: basics of cryptography, encryption and decryption, digital signatures, and secure communication protocols.	Lecture, use of video projector, discussions with students	2
Network Security: firewalls, intrusion detection and prevention systems, virtual private networks (VPNs), risks and vulnerabilities associated with wireless networks.	Lecture, use of video projector, discussions with students	4
Operating System Security: key security features of popular operating systems (Windows and Linux), access control, privilege escalation, and malware protection.	Lecture, use of video projector, discussions with students	2
Web Security: security issues associated with web applications, cross-site scripting (XSS) and SQL injection attacks, web application security frameworks and best practices.	Lecture, use of video projector, discussions with students	4
Mobile Security: security issues associated with mobile devices, mobile app security, mobile device management (MDM), and mobile data protection.	Lecture, use of video projector, discussions with students	2
Cloud Security: security issues associated with cloud computing, data protection, encryption, and secure access management.	Lecture, use of video projector, discussions with students	4
Privacy: privacy laws and regulations, privacy best practices, and privacy- enhancing technologies such as anonymization and differential privacy.	Lecture, use of video projector, discussions with students	2
Incident Response and Forensics: incident response procedures, including the identification, containment, and eradication of security threats, as well as digital forensics and data recovery.	Lecture, use of video projector, discussions with students	2
Ethical Hacking and Penetration Testing: fundamentals of ethical hacking and penetration testing, the use of various tools and techniques to identify vulnerabilities and assess the security of systems and networks.	Lecture, use of video projector, discussions with students	2
Security Management: policies, procedures, and governance structures used to manage security, including risk assessment, security audits, and compliance frameworks.	Lecture, use of video projector, discussions with students	2
	Total lecture hours:	**28**

8.2. Practical activities (8.2.a. Seminar[20]/ 8.2.b. Laboratory[21]/ 8.2.c. Project[22])	**Teaching methods**	**Hours**
Password management: critical aspect of security and privacy.	Use of video projector, discussions with students	2

Phishing simulation: real-life scenarios to create phishing simulations.	Use of video projector, discussions with students	2
Two-factor authentication: an extra layer of security to login credentials.	Use of video projector, discussions with students	2
Physical security: essential to protect sensitive data; using encrypted storage to protect sensitive data.	Use of video projector, discussions with students	4
Safe browsing: Internet browsing can be a security risk.	Use of video projector, discussions with students	2
Data protection: data classification, the importance of data backups, and how to use encryption to secure sensitive data.	Use of video projector, discussions with students	2
Privacy policies: understanding privacy policies, how to opt-out of data collection.	Use of video projector, discussions with students	2
Mobile device security: password protection, app permissions, and safe browsing practices.	Use of video projector, discussions with students	4
Incident response: incident response plan in case of a security breach; how to respond to security incidents.	Use of video projector, discussions with students	4
Social engineering: identify and avoid social engineering scams, such as phishing attempts, phone scams, and fake emails.	Use of video projector, discussions with students	4
Total seminar/laboratory hours:		28

9. Bibliography

9.1. Recommended Bibliography	1. Security and Privacy in the Digital Era, C Guerrier, Hoboken, United States, 2016
9.2. Additional Bibliography	2. Privacy's Blueprint: The Battle to Control the Design of New Technologies,Woodrow Hartzog, 2018

10. Conjunction of the discipline's content with the expectations of the epistemic community, professional associations and significant employers of the specific study program[23]

It is done through regular contacts with the representatives of the companies. Security and privacy topic is an actual topic and is of great interest in existing software companies on the local, national and global market.

11. Evaluation

Activity Type	11.1 Evaluation Criteria	11.2 Evaluation Methods		11.3 Percentage in the Final Grade	Obs.[24]
11.4a Exam / Colloquy	• Theoretical and practical knowledge acquired (quantity, correctness, accuracy)	Tests during the semester[25]:	%	50% (minimum 5)	CEF
		Homework:	%		
		Other activities[26]:	%		
		Final evaluation:	50%		
11.4b Seminar	• Frequency/relevance of participation or responses	Evidence of participation, portfolio of papers (reports, scientific summaries)		5% (minimum 5)	nCPE
11.4c Laboratory	• Knowledge of the equipment, how to use specific tools; evaluation of tools, processing and interpretation of results	• Written questionnaire • Oral response • Laboratory notebook, experimental works, reports, etc. • Practical demonstration		5% (minimum 5)	nCPE
11.4d Project	• The quality of the project, the correctness of the project documentation,	• Self-evaluation, project presentation • Critical evaluation of a project		40% (minimum 5)	nCPE

	the appropriate justification of the chosen solutions			
11.5 Minimum performance standard[27] To pass the exam, the candidate must have a basic knowledge of the security and privacy and knows how to identify possible threats				

The Course Syllabus will encompass components adapted to persons with special educational needs (SEN – people with disabilities and people with high potential), depending on their type and degree, at the level of all curricular elements (skills, objectives, contents, teaching methods, alternative assessment), in order to ensure fair opportunities in the academic training of all students, paying close attention to individual learning needs.

Filling Date: |_1_|_5_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

Department Acceptance Date: |_3_|_0_| / |_0_|_9_| / |_2_|_0_|_2_|_5_|

	Academic Rank, Title, First Name, Last Name	**Signature**
Course Teacher	Professor PhD. Ana-Maria Acu	
Study Program Coordinator	Associated Professor PhD. Nicolae Constantinescu	
Department Head	Professor PhD. Mugur Acu	

[1] *Bachelor / Master*
[2] *1-4 for bachelor, 1-2 for master*
[3] *1-8 for bachelor, 1-3 for master*
[4] *Exam, colloquium or VP A/R - from the curriculum*
[5] *Course type: R = Compulsory course; E = Elective course; O = Optional course*
[6] *Formative category: S = Specialty; F = Fundamental; C = Complementary; I = Fully assisted; P = Partially assisted; N = Unassisted*
[7] *Equal to 14 weeks x number of hours from point 3.1 (similar to 3.2.a.b.c.)*
[8] *The following lines refer to individual study; the total is completed at point 3.37.*
[9] *Between 7 and 14 hours*
[10] *Between 2 and 6 hours*
[11] *The sum of the values from the previous lines, which refer to individual study.*
[12] *The sum (3.5.) between the number of hours of direct teaching activity (NOAD) and the number of hours of individual study (NOSI) must be equal to the number of credits assigned to the discipline (point 3.7) x no. hours per credit (3.6.)*
[13] *The credit number is computed according to the following formula, being rounded to whole neighbouring values (either by subtraction or addition*

$$No.credits = \frac{NOCpSpD \times C_C + NOApSpD \times C_A}{TOCpSdP \times C_C + TOApSdP \times C_A} \times 30\ credits$$

Where:

- NOCpSpD = Number of lecture hours / week / discipline for which the credits are calculated
- NOApSpD = Number of application hours (sem./lab./pro.) / week / discipline for which the credits are calculated
- TOCpSdP = Total number of course hours / week in the Curriculum
- TOApSdP = Total number of application hours (sem./lab./pro.) / week in the Curriculum
- C_C/C_A = Course coefficients / applications calculated according to the table

Coefficients	**Course**	**Applications (S/L/P)**
Bachelor	2	1
Master	2,5	1,5
Bachelor - foreign language	2,5	1,25

[14] *The courses that should have been previously completed or equivalent will be mentioned*
[15] *Board, video projector, flipchart, specific teaching materials, online platforms, etc.*
[16] *Computing technology, software packages, experimental stands, online platforms, etc.*
[17] *Competences from the Grids related to the description of the study program, adapted to the specifics of the discipline*
[18] *Chapter and paragraph titles*
[19] *Exposition, lecture, board presentation of the studied topic, use of video projector, discussions with students (for each chapter, if applicable)*
[20] *Discussions, debates, presentations and/or analyses of papers, solving exercises and problems*
[21] *Practical demonstration, exercise, experiment*
[22] *Case study, demonstration, exercise, error analysis, etc.*
[23] *The relationship with other disciplines, the usefulness of the discipline on the labour market*
[24] *CPE – Conditions Exam Participation; nCPE – Does Not Condition Exam Participation; CEF - Conditions Final Evaluation; N/A – not applicable*
[25] *The number of tests and the weeks in which they will be taken will be specified*
[26] *Scientific circles, professional competitions, etc.*
[27] *The minimum performance standard in the competence grid of the study program is customized to the specifics of the discipline, if applicable*