COURSE OUTLINE

1. Program Data

1.1 Higher education institution	**Transilvania University of Braşov**
1.2 Faculty	**Electrical and Computer Engineering**
1.3 Department	**Electronics & Computers**
1.4 Field of study	**Electronics, Telecommunications and Information Technology Engineering**
1.5 Cycle of studies[1]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Course Data

2.1 Name of the discipline			Cryptography Fundamentals and Application Scenarios					
2.2 Course Activity Holder			Assoc. Prof. dr. ing. Dominic – Mircea KRISTALY					
2.3 Seminar / laboratory / project coordinator			As. Univ. Eng. CHIŞ Alexandru					
2.4 Year of study	I	2.5 Semester	II	2.6 Type of assessment	Is	2.7 Course Status	Content[2]	DS
							Type of attendance[3]	DOB

3. Total estimated time (hours of teaching activity per semester)

3.1 Number of hours per week	**4**	of which: 3.2 course	**2**	3.3 Seminar / laboratory / project	**0/2/0**
3.4 Total hours in the plan education	56	of which: 3.5 course	28	3.6 Seminar / laboratory / project	0/28/0

Time allocation	Hours
Study of textbooks, course material, bibliography and notes	28
Additional documentation in libraries, specialized electronic platforms and field research	28
Preparation of seminars/labs/projects, assignments, papers, portfolios and essays	24
Tutoring	10
Examination	4
Other activities.....	

3.7 Total number of hours of individual study	94
3.8 Total number per semester	150
3.9 Number of credits[4]	5

4. Prerequisites (if applicable)

4.1 Curriculum related	• Programming and programming languages, object-oriented programming, software engineering, and applications in data communications
4.2 Competency-related	•

5. Conditions (if applicable)

5.1 For the development of the course	• Room equipped with multimedia equipment and whiteboard. Capacity of the hall according to the number of students enrolled
5.2 for the development of the seminar/laboratory/project	• For part-time classes: laboratory equipped with workstations (computers) for specific experiments and internet access

6. Specific competences

Professional skills	**C.1 Manage System Security** ***Knowledge*** **R.I.1.2.** Lists cyberattack techniques and implements effective countermeasures **C.3 Implement risk management in ICT** ***Skills*** **R.I.3.4.** Recommend measures to improve your digital security strategy **C.6 Protects ICT devices** ***Knowledge*** **R.I.6.1.** Identifies safety and security measures and takes due account of trust and privacy ***Skills*** **R.I.6.3.** Use tools and methods to maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics, and protection systems such as firewall, antivirus, spam filters. **C.8 Manage compliance with IT security standards** ***Skills*** **R.Q.8.2** Ensures the implementation of relevant practices, standards and information security requirements at industry level.
Transversal competences	

7. Course objectives (results of the specific competences to be acquired)

7.1 General objective of the course	• Acquiring the fundamentals in cryptography that underpin security protocols
7.2 Specific objectives	• Familiarity with the basic concepts, terminologies and technologies used in the field of cybersecurity • To acquire a very clear picture of the skills needed to work in this field.

8. Content

8.1 Course	Teaching methods	Number of hours	Remarks
Fundamentals of mathematics used in cryptography: elements of probability theory, elements of number theory, elliptic curves, generation of prime numbers	Heuristic conversation, problematization	4	
Introduction to cryptography: basic concepts; the principle of least privilege; the CIA principle (confidentiality, integrity, availability); Authentication methods	Heuristic conversation, problematization	2	
Types of ciphers. Cryptographic features	Heuristic conversation, problematization	2	
Symmetric Cryptographic Key Generation: Random Keys and Pseudo-Random Keys	Heuristic conversation, problematization	2	
Public infrastructures with cryptographic keys	Heuristic conversation, problematization	2	
Symmetric encryption	Heuristic conversation, problematization	2	
Asymmetric encryption	Heuristic conversation, problematization	2	
Key distribution, digital certificates, electronic signature	Heuristic conversation, problematization	2	

Cryptographic Protocols	Heuristic conversation, problematization	2	
Authentication protocols. Information authentication, entity authentication, and authenticated secret key exchanges	Heuristic conversation, problematization	4	
Security of cryptographic feature implementations	Heuristic conversation, problematization	4	

Bibliography

1. Groza Bogdan, Introduction to Cryptography: Cryptographic Functions, Mathematical and Computational Foundations, Politehnica Publishing House, Timisoara, ISBN 978-606-554-499-4, 200 p., 2012
2. Dan Boneh, Victor Shoup, "A Postgraduate Course in Applied Cryptography", September 2017. Online: http://toc.cryptobook.us/

8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Remarks
Introduction to cryptography – substitution ciphers	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
Pseudo-random number generation laboratory	Demonstration, Experiment, Direct Actions, Problematization, Case Study	4	
One-way cryptographic functions and collision attack	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
Symmetric encryption, block encryption	Demonstration, Experiment, Direct Actions, Problematization, Case Study	4	
RSA Public Key Encryption and Signature Lab	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
Public Key Infrastructure Lab	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
SSL/TLS Protocol	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
Introduction to Steganography	Demonstration, Experiment, Direct Actions, Problematization, Case Study	2	
Introduction to Blockchain	Demonstration, Experiment, Direct Actions, Problematization, Case Study	4	
Exercises Demonstrating Attacks on Real-World Crypto Systems and Applications	Demonstration, Experiment, Direct Actions, Problematization, Case Study	4	

Bibliography
1. Groza Bogdan, Introduction to Cryptography: Cryptographic Functions, Mathematical and Computational Foundations, Politehnica Publishing House, Timisoara, ISBN 978-606-554-499-4, 200 p., 2012
2. Dan Boneh, Victor Shoup, "A Postgraduate Course in Applied Cryptography", September 2017. Online: http://toc.cryptobook.us/

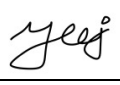
9. Correlation of the course content with the requirements of the labor market (epistemic communities, professional associations, potential employers in the field of study)

In this course, students will become familiar with the basic concepts, terminology, and technologies used in the field of cybersecurity, and gain a clear picture of the skills required to work in this field. The course is basically a beginner's guide for those interested in the topic of cybersecurity, without the need for a very rich technical training.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of final grade
10.4 Course	1. The ability to recognize requirements and correctly solve application problems based on formulas and procedures. 2. Ability to apply the knowledge gained to address new situations, to carry out analyses and comparisons 3. Clarity, consistency, conciseness of the presentation and functional explanation.	Written exam	40%
		Summative evaluation on Journey	10%
10.5 Seminar/ laboratory/ project	Degree of involvement in practical activity. Attitude towards practical activity. Participation in debates; Initiative; Attitudes related to this problem, teachers and colleagues.	Direct observation. Directional questions. Formative assessment, on the way.	20%
	The ability to understand the requirements. Ability to solve requirements independently;	The colloquium consists of the presentation of the practical results and the analysis of the implementation. The grading scale is explicit and is transmitted to the students with the given requirements	30%
10.6 Minimum Performance Standard			
R.I.1.2. Lists cyberattack techniques and implements effective countermeasures **R.I.3.4.** Recommend measures to improve your digital security strategy **R.I.6.1.** Identifies safety and security measures and takes due account of trust and privacy **R.I.6.3.** Use tools and methods to maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics, and protection systems such as firewall, antivirus, spam filters. **R.Q.8.2** Ensures the implementation of relevant practices, standards and information security requirements at industry level.			

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) Assoc. Prof. Dominic – Mircea KRISTALY	(Name, Surname, Signature of seminar/laboratory/project holder) As.Univ. Eng. CHIȘ Alexandru 
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

1. Field of study - one of the following options is chosen: Bachelor's / Master's / Doctorate (to be completed according to the Nomenclature of fields and specializations/ university study programs in force);
2. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
3. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
4. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);
5. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course			Types of Cyberattacks and Threats					
2.2 Course convenor			BĂLAN Titus Constantin					
2.3 Seminar/ laboratory/ project convenor			ŞOLCĂ Robert-Nicolae					
2.4 Study year	1	2.5 Semester	1	2.6 Evaluation type	E	2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**2**	out of which: 3.2 lecture	**1**	3.3 seminar/ laboratory/ project	**0/1/0**
3.4 Total number of hours in the curriculum	28	out of which: 3.5 lecture	14	3.6 seminar/ laboratory/ project	0/14/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	28
Additional documentation in libraries, specialized electronic platforms, and field research	24
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	28
Tutorial	8
Examinations	4
Other activities.....	

3.7 Total number of individual study hours	92
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Programming languages, Object Oriented Programming, Software Engineering and Communications
4.2 competences-related	• C.1 Manages system security • C.3 Implements ICT risk management • C.6 Protects ICT devices

5. Conditions (if applicable)

5.1 for course development	• Room equipped with multimedia equipment and white board. Room capacity according with the number of registered students
5.2 for seminar/ laboratory/ project development	• For tutoring at partially assisted hours: laboratory equipped with workstations (computers) for specific experiments and Internet access

6. Specific competences

Professional competences	**C.1 Manages system security**; L.R.1.2. Enumerates cyber-attack techniques and implements effective countermeasures; L.R.1.4. Analyzes an organization's critical assets and identifies weaknesses and vulnerabilities that could lead to intrusion or attack. **C.3 Implements ICT risk management**; L.R.3.1. Identifies opportunities to mitigate cyber security risks. **C.6 Protects ICT devices**; L.R.6.4. Demonstrates initiative and proactive behavior in updating professional knowledge in software and hardware security to maximize the safety of computing devices.
Transversal competences	CT1 Responsible execution of professional tasks, respecting the moral and ethical values, in conditions of autonomy and professional independence, with practical applicability and responsibility for the activities undertaken, in the perspective of Integrating electronic, computing and communications systems with the environment - social, legislative, administrative and ecological – in the terms of sustainable development.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Development and strengthening of the competencies required to manage the security of information systems and associated risks by identifying critical assets, assessing vulnerabilities, and applying effective countermeasures to protect the ICT infrastructure.
7.2 Specific objectives	• Enumeration and comprehension of cyber-attack techniques and the application of effective countermeasures. • Analysis of an enterprise's critical assets to identify weaknesses and vulnerabilities that could lead to attacks. • Identification and assessment of opportunities to reduce cyber-security risks. • Demonstration of initiative and autonomy in continuously updating professional knowledge in software and hardware security to maximize the safety of ICT devices. • Responsible execution of professional tasks with adherence to moral and ethical principles, assuming accountability in integrating electronic, computing, and communication systems within social, legislative, and administrative contexts for sustainable development.

8. Content

8.1 Course	Teaching methods	Number of hours	Remarks
Introduction – security attack definition, common cyber-security attacks – stages and patterns	Heuristic conversation, Problematization, Case study	4	

Types of cyber attacks, vulnerabilites of security systems. Classification of cyber security attacks: Device compromise attacks, Service Disruption Attacks, Data Exfiltrations Attacks, Bad Data Injections, Advanced persistent threats.	Heuristic conversation, Problematization, Case study	2	
Device compromise attacks. Use cases.	Heuristic conversation, Problematization, Case study	3	
Service Disruption Attacks. Use cases.	Heuristic conversation, Problematization, Case study	3	
Data Exfiltrations Attacks. Use cases.	Heuristic conversation, Problematization, Case study	3	
Bad Data Injections. Use cases.	Heuristic conversation, Problematization, Case study	3	
Advanced persistent threats. Use cases.	Heuristic conversation, Problematization, Case study	3	
Methods of prevention against security attacks	Heuristic conversation, Problematization, Case study	3	
Use case - Antivirus	Heuristic conversation, Problematization, Case study	2	
Bibliography 1. Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice, 4th Edition; Pearson Education, ISBN 978-0134794105 2. Hansman, S., & Hunt, R. (2005). A Taxonomy of Network and Computer Attacks; Computers & Security, Vol. 24(1), pp. 31–43, DOI: 10.1016/j.cose.2004.06.005. 3. Alazab, M., & Venkataraman, S. (2019). Advanced Persistent Threats: Detection, Prevention and Forensics; Springer Nature, ISBN 978-3030219770			
8.2 Seminar/ laboratory/ project	Teaching-learning methods	Remarks	
Drive-by exploits (Java by Drive, etc.) Trojans / Malicious code	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Sql Injection attack	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Botnet/Apt Denial of Service (Dos, DDos) attack	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Phishing attack	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Attack based on information leakeage	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Security attacks based on search engine	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
PKI vulnerabilities (man in the middle attack); compromised digital certificates	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Arbitrary Code Execution/Remote Code Execution	Demonstration, Experiment, Direct actions, Problematization, Casestudy	1	
Bibliography 1. Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice, 4th Edition; Pearson Education, ISBN 978-0134794105 2. Hansman, S., & Hunt, R. (2005). A Taxonomy of Network and Computer Attacks; Computers & Security, Vol. 24(1), pp. 31–43, DOI: 10.1016/j.cose.2004.06.005. 3. Alazab, M., & Venkataraman, S. (2019). Advanced Persistent Threats: Detection, Prevention and Forensics; Springer Nature, ISBN 978-3030219770			

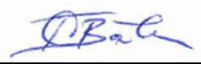
9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

The course provides an overview of the security vulnerabilities that may arise in a computer system as well as a classification and description of the types of existing attacks accompanied by real-world examples.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	1. The ability to recognize the requirements and to correctly solve applicative problems based on formulas and procedures. 2. The ability to apply the accumulated knowledge to approach new situations, to carry out analyses and comparisons 3. Clarity, consistency, brevity of exposure and functional explanation.	Written examination	40%
		Active attendance	10%
10.5 Seminar/ laboratory/ project	Degree of involvement in the practical activity; Attitude towards the practical activity. Participation in debates; Innitiative; Attitudes relative to the matter, teachers and colleagues.	Direct observation. Directioned questioning. Formative evaluation, on the way.	20%
	The capacity to understand the requirements; Ability to resolve the requirements independently;	The colloquium consists in presenting the practical results, and analyzing the implementation.	30%
10.6 Minimal performance standard			
• (R.Î.1.2) Enumerates the main cyber-attack techniques and implements a basic countermeasure for each. • (R.Î.1.4) Identifies and classifies at least two critical assets of an enterprise and describes at least two vulnerabilities associated with each. • (R.Î.3.1) Draws up a minimum list of three preventive measures to reduce cyber-security risks. • (R.Î.6.4) Demonstrates initiative by documenting and implementing a monthly update procedure for software and firmware packages on an ICT device.			

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course convenor) BĂLAN Titus Constantin 	(Last name, First name, signature of seminar/ laboratory/ project convenor) ȘOLCĂ Robert-Nicolae ……
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

1) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

2) Study level – choose from among: BA/MA/PhD;

3) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

4) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

5) One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Program data

1.1 Institution of higher education	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics & Computers
1.4 Master 's field of study 1)	Electronics, Telecommunications and Information Technologies
1.5 Cycle of studies2)	Master
1.6 Curriculum/Qualification	Cybersecurity

2. Discipline data

2.1 Name of the discipline	Ethics and academic integrity							
2.2 Course Activity Holder				Conf.dr.ing. Catalin Petrea ION				
2.3 Owner of seminar/laboratory/project activities								
2.4 Year of study	I	2.5 Semester	I	2.6 Type of assessment	C	2.7 Discipline regime	Content3)	DAP
							Obligation3)	**DI**

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**1**	of which: 3.2 course	**1**	3.3 Seminar/ Laboratory/ Project	**0**
3.4 Total hours in the curriculum	**14**	of which: 3.5 course	**14**	3.6 Seminar/ Laboratory/ Project	**0**

Distribution of the time fund	Hours
Study by textbook, course material, bibliography and notes	**20**
Additional documentation in the library, on specialized electronic platforms and in the field	**20**
Preparation of seminars/laboratories/projects, assignments, papers, portfolios and essays	**0**
Tutoring	**4**
Examination	**2**
Other activities	**0**

3.7 Total hours of student activity	**46**
3.8 Total hours per semester	**60**
3.9 Number of credits5)	**2**

4. Preconditions (where applicable)

4.1 Curriculum	
4.2 Competence	

5. Conditions (where applicable)

5.1 Course Conduct	• Classroom with a minimum of 30 seats • Projector
5.2 Conduct of the seminar/laboratory/project	

6. Specific skills accumulated (according to the skills grid in the curriculum)

Professional skills	

Transversal competence	CT1. Responsible execution of professional tasks, in compliance with moral and ethical values, in conditions of professional autonomy and independence, with practical applicability and with the assumption of responsibility for the activities undertaken in the spirit of integration of electrical and advanced systems in the environment, in conditions of sustainable development.

7. Objectives of the discipline (resulting from the specific skills accumulated)

7.1 General objective of the discipline	*Developing knowledge about ethics and integrity in scientific activity*
7.2 Specific objectives	Knowledge of the rules of ethics and integrity in scientific activity Understanding the principles of writing an integral academic paper Acquiring the deontological principles regarding teamwork

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Introductory notions of ethics and integrity in scientific activity	Presentation with projector. Discussion.	2	
Regulations on ethics in scientific and research activity	Presentation with projector. Discussion.	2	
Principles of writing an integral academic paper	Presentation with projector. Discussion.	2	
Ethics in citation. Search for references, ways to cite	Presentation with projector. Demonstrations.	2	
Plagiarism, self-plagiarism and other associated problems. Identification and prevention	Presentation with projector. Demonstrations.	2	
Professional deontology in teamwork. Principles, legislation, challenges	Presentation with projector. Discussion.	2	
Responsibility related to the results of the research. Risks, precautions and limits	Presentation with projector. Demonstrations.	2	

Bibliography

1. Gail Baura, Engineering Ethics, 1st Edition, An Industrial Perspective ISBN: 9780080458021, available at the Unitbv library
2. Liliana Rogozea, s.a., Guide to Good Practices in Academic Research, https://elearning.unitbv.ro/course/view.php?id=3414
3. Edwards, M. A., & Roy, S. (2017). Academic research in the 21st century: Maintaining scientific integrity in a climate of perverse incentives and hypercompetition. Environmental Engineering Science, 34(1), 51-61, https://www.liebertpub.com/doi/full/10.1089/ees.2016.0223
4. Practical Guide on Ethics in Scientific Research, PODCA Project, 2013. http://date-cdi.ro/sites/default/files//uploads/1.%20ghid%20privind%20etica%20%C3%AEn%20cercetarea%20%C8%99tiin%C8%9Bific%C4%83%20.pdf
5. J. H. Moor, Why we need better ethics for emerging technologies, Ethics and Information Technology (2005) 7:111–119.
6. Law no. Law no. 206/2004 (updated) on good conduct in scientific research, technological development and innovation.

9. Corroborating the contents of the discipline with the expectations of the representatives of the epistemic communities, of the professional associations and of the representative employers in the field related to the program

European regulations and those recommended by the IEEE professional association (www.ieee.org) are taken into account.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight of the final grade
10.4 Course	Ability to explain the rules of ethics and academic integrity	Colloquium	80%
	The degree of involvement in debates, discussions, realization of homework.	Evaluation during the semester.	20%

	Presence	No. of attendance/Total number of courses	Max. bonus 1p
10.6 Minimum Performance Standard			
LR Knowledge of the basic rules and values related to ethics and academic integrity			

This Disciplinary Sheet was approved in the meeting of the Department Council on ..../...../.... and approved in the meeting of the Faculty Council on ..../...../.....

Conf.dr.ing. Titus BALAN ..... . Dean	**Head of dr.ing. Cornel Aurel STANCA** ..... Department Director
Assoc. Prof. Dr. Catalin Petrea ION, ... Course holder	

Note:

[6)] Field of study - choose one of the following variants: Bachelor's/Master's/Doctorate (to be filled in according to the Nomenclature of fields and specializations/university study programs in force);

[7)] The study cycle - one of the following variants is chosen: Bachelor's/ Master's/ Doctorate;

[8)] Discipline regime (content) - one of the variants is chosen: **DF** (fundamental discipline)/ **DD** (discipline in the field)/ **DS** (specialized discipline)/ **DC** (complementary discipline) - for the bachelor's level; **DAP** (deepening discipline)/ **DSI** (synthesis discipline)/ **DCA** (advanced knowledge discipline) - for the master's level;

[9)] Discipline regime (compulsory) - one of the variants is chosen: **DI** (compulsory subject)/ **DO** (optional subject)/ **DFac** (optional subject);

[10)] One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

DISCIPLINE SHEET

1. Program Data

1.1 Higher education institution	**Transilvania University of Brașov**
1.2 Faculty	**Electrical Engineering and Computer Science**
1.3 Department	**Electronics & Computers**
1.4 Field of Master's studies1)	**Electronic Engineering, Telecommunications and Information Technology**
1.5 Cycle of studies[2)]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Data about the discipline

2.1 Name of the discipline	**Practice**							
2.2 Course Activity Holder								
2.3 Holder of seminar/laboratory/project activities	Prof. dr. ing. Titus-Constantin BĂLAN							
2.4 Year of study	**I**	2.5 Semester	**I**	2.6 Type of assessment	**C**	2.7 Discipline regime	Contents3)	**DS**
							Obligation3)	**DOB**

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**10**	of which: 3.2 course	**0**	3.3 Seminar / Laboratory / Project	**0/0/10**
3.4 Total hours in the curriculum	**140**	of which: 3.5 course	**0**	3.6 Seminar/ laboratory/ project	**0/0/140**

Partially assisted activities – 10 hours/week	
Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	0
Additional documentation in the library, on specialized electronic platforms and in the field	0
Preparation of seminars / laboratories / projects, assignments, reports, portfolios and essays	0
Tutoring	0
Examination	0
Other activities.....	70

3.7 Total hours of individual study	70
3.8 Total hours per semester	210
3.9 Number of credits5)	7

4. Preconditions (where applicable)

4.1 Curriculum	• This is not the case
4.2 Competencies	• This is not the case

5. Conditions (where applicable)

5.1 Course Schedule	• This is not the case
5.2 Conducting the seminar/laboratory/project	• University laboratories and activity at economic partners • Conditions according to the internship agreement between the university and partners

6. Specific skills acquired (according to the competence grid in the curriculum)

Professional skills	**C.1 Manage System Security** ***Skills*** **R.I.1.3.** Apply detection techniques for security **C.2 Define security policies** ***Skills*** **R.I.2.2.** Designs and executes a set of written rules and policies that aim to ensure an organization in terms of constraints related to stakeholder behavior, mechanical protection constraints, and constraints related to data access **C.3 Implement risk management in ICT** ***Skills*** **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy **C.6 Protects ICT devices** ***Skills*** **R.I.6.3**. Use tools and methods to maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics, and protection systems such as firewall, antivirus, spam filters. ***Responsibility and autonomy*** **R.I.6.4.** Show initiative and action to update professional knowledge in the field of software and hardware security, maximizing the security of computing devices
Transversal competences	

7. Objectives of the discipline (resulting from the specific competences acquired)

7.1 General objective of the discipline	Guiding students in carrying out applied and research projects completed by participating in conferences, scientific communication sessions or articles published in specialized journals
7.2 Specific objectives	• encouraging students to develop research ideas • engaging students in individual research projects or in partnership with agents from the industrial environment • correct writing of a scientific paper, according to the required templates

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Bibliography			
8.2 Seminar/ laboratory/ project Partially assisted activities	Teaching-learning methods	Number of hours	Observations
	Brainstorming discussions to identify topics of interest. Encouraging teamwork. Presentation of examples from the field of interest.	10 hours per week	
Bibliography Bibliography [1]. OPTIM http://www.info-optim.ro/authors_kit.php Conference [2]. Bulletin of the Transilvania University of Braşov http://webbut.unitbv.ro/bulletin/Series%20I/Instructions.html			

9. Corroboration of the contents of the discipline with the expectations of the representatives of the epistemic communities, professional associations and representative employers in the field related to the program

Employers' expectations were identified with an important weight in the direction of developing theoretical and practical research skills and applying general knowledge in modern applications.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final grade
10.4 Course			
10.5 Seminar/ laboratory/ project	Research topic in the field of master's specialization	Final evaluation with the presentation of the results of each paper	10%
	Scientific level/degree of interest for agents in the industrial environment		40%
	Degree of novelty / usefulness		10%
	Clarity, coherence, conciseness of the presentation and Explanation of the functionality Work	Evaluation along the way with presentation of phased results	30%
	Presentation of the paper at a conference, scientific communications session or publication in a specialized journal	Acceptance of the paper for support or publication.	10%
10.6 Minimum Performance Standard			
Minimum objectives: **R.I.1.3.** Apply detection techniques for security **R.I.2.2.** Be able to design and implement a set of written rules and policies that aim to ensure an organisation in terms of constraints related to stakeholder behaviour, mechanical protection constraints and constraints related to data access **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy			

R.I.6.3. Use tools and methods that maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics and protection systems such as firewall, antivirus, spam filters **R.I.6.4.** Maximize the security of computing devices

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) BĂLAN Titus Constantin	(Name, Surname, Signature of seminar/laboratory/project holder) BĂLAN Titus Constantin
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

6. Field of study - one of the following options is chosen: Bachelor's degree/ Master's degree/ Doctorate (to be completed according to the Nomenclature of fields and specializations/university study programs in force);
7. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
8. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
9. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);
10. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Program data

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics & Computers
1.4 Field of study ..... [1)]	Electronic Engineering, Telecommunications and Information Technology
1.5 Cycle of studies[2)]	Masters
1.6 Curriculum/Qualification	Cybersecurity

2. Discipline data

2.1 Name of the discipline	Cybersecurity incident management							
2.2 Course Activity Holder	Head of work. Dr. ing. CARP Marius							
2.3 Owner of seminar/laboratory/project activities	Head of work. Dr. ing. CARP Marius							
2.4 Year of study		2.5 Semester		2.6 Type of assessment		2.7 Discipline regime	Content3)	SC
							Obligation3)	CPC

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**3**	of which: 3.2 course	**1**	3.3 Seminar/ Laboratory/ Project	**0/1/1**
3.4 Total hours of the curriculum	42	of which: 3.5 course	14	3.6 Seminar/ Laboratory/ Project	0/14/14

Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	25
Additional documentation in the library, on specialized electronic platforms and in the field	25
Preparation of seminars/laboratories/projects, assignments, papers, portfolios and essays	14
Tutoring	10
Examination	4
Other activities.....	

3.7 Total hours of individual study	78
3.8 Total hours per semester	120
3.9 Number of credits[5)]	4

4. Preconditions (where applicable)

4.1 Curriculum	• Knowledge of security of computer networks and information systems
4.2 Competences	•

5. Conditions (where applicable)

5.1 Course Conduct	• Classroom with a minimum of 30 seats, • Projector • Board.
5.2 Conduct of the seminar/laboratory/project	• Laboratory with individual computers

6. Specific skills accumulated (according to the skills grid in the curriculum)

Professional skills	C1 - Manages the security of the system; Lists cyberattack techniques and implements effective countermeasures; Apply detection techniques for security; It analyzes a company's critical assets and identifies weaknesses and vulnerabilities that led to the intrusion or attack. Carry out processes in the management of cybersecurity projects, taking on different roles in the team and describing clearly and concisely, verbally and in writing, the results. C3 – Implements ICT risk management; Identifies opportunities to mitigate cybersecurity risks; Develops and implements procedures for identifying, assessing, treating and mitigating ICT risks, such as unauthorized access or data leaks, in accordance with the company's risk strategy, procedures and policies; Analyzes and manages security risks and incidents; Recommends measures to improve the digital security strategy C5 - Manages compliance with IT security standards; List information security practices, standards, and requirements; Ensures the implementation of relevant industry information security practices, standards and requirements. It shows a spirit of initiative and action to guide the implementation of measures and requirements in the field of information security. C6 - Protects ICT devices; Identifying safety and security measures and taking due account of trust and confidentiality; Protects ICT devices and digital content and understands the risks and threats in digital environments; Use tools and methods to maximize the security of ICT devices and information through access control such as passwords, digital signatures, biometrics, and protection systems such as firewalls, antivirus, spam filters
Transversal competences	CT1 - Problem solving; Develop problem-solving strategies; Find solutions to problems; Apply various strategies to solve problems

7. Objectives of the discipline (resulting from the specific skills accumulated)

7.1 General objective of the discipline	The course presents the essential steps of collecting security events from the security technologies implemented within an infrastructure, along with the mechanisms and tools for monitoring and analyzing incidents.
7.2 Specific objectives	Understanding and acquiring the principles underlying a SIEM/SOC Planning and design of SOC systems as well as the acquisition and ability to implement specific methods: • Security Log Collection • Security log aggregation and parsing • Security log storage • Alerting and analysis strategies • Analysis of important network services (email, DNS, HTTP, HTTPS) with the help of SIEM/SOC • Security incident management at SIEM/SOC level • Software monitoring • Traffic monitoring • User behavior analysis • Post-detection analysis

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations

Introduction to Cyber Defense Description Kill Chain (stages of an attack) Traditional attacks vs. modem attacks Presentation of infection vectors.	Heuristic Conversation, Problematization, Case Study	2	
Security architecture of cyber infrastructures Description of the following security technologies and presentation of their role in securing infrastructures from a cibemetic point of view. • Router Switch Firewall WAF NIDS/NIPS UTM/NGFW • Sandbox Proxy SIEM/SOC • Packet capture • Honeypot • Threat intelligence	Heuristic Conversation, Problematization, Case Study	2	
The architecture and principles underlying a SIEM/SOC Planning & Concept Security Log Collection Security log aggregation and parsing Security log storage Alerting and analysis strategies	Heuristic Conversation, Problematization, Case Study	4	
Analysis of important network services (email, DNS, HTTP, HTTPS) with the help of SIEM/SOC	Heuristic Conversation, Problematization, Case Study	2	
Advanced endpoint analytics Collection strategies Endpoint Securing - Patching, Whitelisting, Blacklisting, AV, HIDS, HIPS, User Rights Control Log collection in various operating systems Authentication. Methods for identifying malware Monitoring of registers and processes Firewall services (host - based) at the level of operating systems and event logging.	Heuristic Conversation, Problematization, Case Study	2	
Security incident management at SIEM/SOC level Software monitoring Scripting	Heuristic Conversation, Problematization, Case Study	2	

Traffic monitoring External analysis tools User behavior analysis Post-detection analysis			

Bibliography

1. Gerald L. Kovacich, The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program, Third Edition, Elsevier
2. David Kim, Michael G. Solomon, Fundamentals Of Information Systems Security (Information Systems Security & Assurance)
3. Omar Santos, John Stuppi, CCNA Security 210-260 Official Cert Guide Published Sep 1, 2015 by Cisco Press
4. Hacking Exposed 7: Network Security Secrets and Solutions 7th Edition
5. Limor Elbaz et.al, Essentials of Enterprise Network Security: InfoSec pros layout the basics for protecting networks (Peerlyst Presents)
6. Comptia Security+, Authorized Cert Guide, SYO-401, Third Edition

8.2 Laboratory	Teaching-learning methods	Number of hours	Observations
Analysis of important network services (email, DNS, HTTP, HTTPS) with the help of SIEM/SOC	Demonstration, Experiment, Direct Actions, Case Studies	4	
Advanced endpoint analytics a Collection strategies a Endpoint Securing - Patching, Whitelisting, Blacklisting, AV, HIDS, HIPS, User Rights Control a Collection of logs in various operating systems Authentication. Methods of identifying malware Monitoring of registries and processes a Firewall services (host - based) at the level of operating systems and event logging.	Demonstration, Experiment, Direct Actions, Case Studies	6	
Security incident management at SIEM/SOC level a Software monitoring a Scripting a Traffic monitoring a External analysis tools User behavior analysis Post-detection analysis	Demonstration, Experiment, Direct Actions, Case Studies	4	
8.3 Project	Teaching-learning methods	Number of hours	Observations

Students will need to plan and build a SOC center for security incident management; The methodology for dealing with incidents and tools used in the laboratory will be used. The student will act as a manager for dealing with incidents.	Lecture / exemplification / project status check and individual work	14	

Bibliography

1. Gerald L. Kovacich, The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program, Third Edition, Elsevier
2. David Kim, Michael G. Solomon, Fundamentals Of Information Systems Security (Information Systems Security & Assurance)
3. Omar Santos, John Stuppi, CCNA Security 210-260 Official Cert Guide Published Sep 1, 2015 by Cisco Press
4. Hacking Exposed 7: Network Security Secrets and Solutions 7th Edition
5. Limor Elbaz et.al, Essentials of Enterprise Network Security: InfoSec pros layout the basics for protecting networks (Peerlyst Presents)
6. Comptia Security+, Authorized Cert Guide, SYO-401, Third Edition

9. To corroborate the contents of the discipline with the expectations of the representatives of the epistemic communities, of the professional associations and of the representative employers in the field related to the program

The field of cyber security has started to take on new dimensions with the increase in the degree of automation of the technological level and the expansion and amplification of cyber threats/attacks.

Security administrators in any organization have the difficult task of trying to cope with all the cyber threats they face and minimizing the possibilities of compromising their IT infrastructure. In this regard, it is necessary to optimize the process of monitoring security events, in order to prevent, detect and respond to cyber security incidents.

10. Evaluation

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight of the final grade
10.4 Course	Knowledge of concepts; Understanding phenomena; Ability to apply the accumulated knowledge; Ability to understand and fundamental cryptographic notions Ability to analyze and understand cryptographic protocols	Written exam *The grading scale is explicit and is made known from the beginning of the semester*	40%

	Language appropriate to the discipline;		
	Knowledge of concepts; Understanding phenomena; Ability to apply the accumulated knowledge; Ability to understand and fundamental cryptographic notions Ability to analyze and understand cryptographic protocols Language appropriate to the discipline;	Half-semester written exam *The grading scale is explicit and is made known from the beginning of the semester*	10%
10.5 Seminar / laboratory / project	Participation in debates Initiatives Attitude towards learning, towards the course, teacher, colleagues	Direct observation Rhetorical questions and directed questions, etc.	10%
	The degree of involvement in the conduct of the experiments, Attitude towards laboratory activities; Ability to understand phenomena	Direct observation, Sample questions, etc.	40%
10.6 Minimum Performance Standard			
• R.Î.1.5. Performs processes in cybersecurity project management, taking on different roles in the team and clearly and concisely describing the results, verbally and in writing. • R.Î.3.2. Develops and implements procedures for identifying, assessing, treating and mitigating ICT risks, such as unauthorized access or data leaks, in accordance with the company's risk strategy, procedures and policies • R.Î.4.1. Identifies and collects potential critical issues and recommends solutions based on the necessary standards and solutions • R.Î.8.2. Remediates cloud-related issues and establishes ways to restore operations • R.Î.11.2. Updates the methodology that contains measures to ensure that an organization's units can continue to function in the event of a wide range of unforeseen events			

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of dean)

BĂLAN Titus Constantin

Course holder

Head of work. Dr. ing. Marius CARP

(Last name, First name, signature of head of department)

STANCA Aurel Cornel

Seminar / laboratory / project holder

Head of work. Dr. ing. Marius CARP

Note:

1) Field of study - choose one of the following variants: Bachelor's/Master's/Doctorate (to be filled in according to the Nomenclature of fields and specializations/university study programs in force);

2) The study cycle - one of the following variants is chosen: Bachelor's/ Master's/ Doctorate;

3) Discipline regime (content) - one of the variants is chosen: **DF** (fundamental discipline)/ **DD** (discipline in the field)/ **DS** (specialized discipline)/ **DC** (complementary discipline) - for the bachelor's level; **DAP** (deepening discipline)/ **DSI** (synthesis discipline)/ **DCA** (advanced knowledge discipline) - for the master's level;

4) Discipline regime (compulsory) - one of the variants is chosen: **DI** (compulsory subject)/ **DO** (optional subject)/ **DFac** (optional subject);

5) One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course				Business Process Management				
2.2 Course convenor				Conf.dr.ing. Liviu PERNIU				
2.3 Seminar/ laboratory/ project convenor				Conf.dr.ing. Liviu PERNIU				
2.4 Study year		2.5 Semester		2.6 Evaluation type		2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**1**	out of which: 3.2 lecture	**1**	3.3 seminar/ laboratory/ project	**0/0/0**
3.4 Total number of hours in the curriculum	28	out of which: 3.5 lecture	14	3.6 seminar/ laboratory/ project	0/0/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	12
Additional documentation in libraries, specialized electronic platforms, and field research	14
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	20
Tutorial	14
Examinations	2
Other activities.....	

3.7 Total number of individual study hours	62
3.8 Total number per semester	90
3.9 Number of credits[5)]	3

4. Prerequisites (if applicable)

4.1 curriculum-related	• Computer Programming and Programming Languages; Software Engineering and Applications in Data Communications
4.2 competences-related	• C.4 Conducts ICT audits • C.5 Manages compliance with IT security standards • C.8 Develops information security strategy • C.13 Demonstrates entrepreneurial spirit

5. Conditions (if applicable)

5.1 for course development	• video projector
5.2 for seminar/ laboratory/ project development	• computer network • virtual machines • specialized programs

6. Specific competences

Professional competences	**C.4 Conducts ICT audits;** L.R.4.3. Manages processes in cybersecurity project management, assuming various team roles and clearly and concisely communicating results both orally and in writing. **C.5 Manages compliance with IT security standards;** L.R.5.1. Lists information security practices, standards, and requirements. **C.8 Develops information security strategy;** L.R.9.1. Defines cybersecurity strategies.

Transversal competences	**C.13 Demonstrates entrepreneurial spirit;** L.R.13.1. Analyzes business processes based on cost–benefit ratios of a project, using the budget of an existing company or a hypothetical own enterprise.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Development of the competencies required to plan, audit, and implement cybersecurity measures in the ICT environment, ensuring compliance with international standards and the ability to assess the economic feasibility of security projects.
7.2 Specific objectives	• Execution of cybersecurity project management processes, assuming key team roles and communicating results clearly and concisely, both verbally and in writing. • Identification and application of information security practices, requirements, and standards relevant to the organization. • Definition of a comprehensive cybersecurity strategy that includes objectives, necessary resources, and effective implementation mechanisms. • Analysis of business processes based on cost–benefit ratios of security projects, using the budget of an organization or a self-initiated venture to inform investment decisions.

8. Content

8.1 Course	Teaching methods	Remarks
1. Introduction to software systems modeling. Application modeling. Modeling process flows. Service-oriented modeling. Data modeling.	Exercise the use of the index of terms. The conversation / dialog method. Using video recordings and presentations. The conversation / dialog method.	2
2. Process life cycle management. Model of Process Simulation Analysis.		2
3. Compatible assembly models based on components.		2
4. Using domain rules in service-oriented architecture.		2
5. The language used to specify Web services.		2
6. Service-oriented and component-based architecture.		2
7. Security and governance of service-oriented architecture		2

Bibliography

1. Business Process Management, Ueli Wahli, ITSO San Jose/Raleigh, 2007
2. Process choreography and business state machines – http://www.ibm.com/developerworks/webservices/library/ws-soa-progmodel3/index.html
3. OASIS Web Services Business Process Execution Language (WSBPEL) Technical Committee: WS-BPEL 2.0 specification– http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsbpel
4. Open SOA, Service Component Architecture Specifications, http://www.osoa.org/

8.2 Seminar/ laboratory/ project	Teaching-learning methods	Remarks

1. Create a process model	Conversation,	4
2. Developing a component-based architecture	Demonstration,	4
3. Development and management of processes	Case studies,	4
4. Security and governance of service-oriented architecture	Evaluation.	2

Bibliography

1. Business Process Management, Ueli Wahli, ITSO San Jose/Raleigh, 2007
2. Process choreography and business state machines – http://www.ibm.com/developerworks/webservices/library/ws-soa-progmodel3/index.html
3. OASIS Web Services Business Process Execution Language (WSBPEL) Technical Committee: WS-BPEL 2.0 specification–http://www.oasis-open.org/committees/documents.php?wg_abbrev=wsbpel
4. Open SOA, Service Component Architecture Specifications, http://www.osoa.org/

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

The content of the discipline belongs to the field of applied informatics and is meant for information and communication technology in the analysis, synthesis and evaluation of data. Data handling is applicable to any field of activity that uses electronic means of operation.

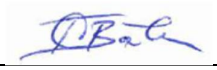
10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	The quality of the evaluation achieved by analyzing, synthesizing, generalizing the data obtained through its own investigation	Summative assessment (written exam evaluation method) - traditional theoretical knowledge test	40%
	Quality of judgments, logical thinking, flexibility	Formal evaluation - assessment during the course	30%
10.5 Seminar/ laboratory/ project	Quality of judgments, logical thinking, flexibility	Summative assessment - assessment by practice - on the computer. Final test	30%

10.6 Minimal performance standard

- The final exam average is calculated only if the grade obtained in the theoretical test and the grade obtained at the practical test (according to the scales initially announced) are at least 5.
- (R.Î.4.3) Plans and manages a minimal cybersecurity project lifecycle in a team setting.
- (R.Î.5.1) Identifies and lists at least three relevant information security standards and requirements.
- (R.Î.8.1) Drafts a concise cybersecurity strategy document containing at least three specific objectives and two implementation mechanisms.
- (R.Î.13.1) Conducts a cost–benefit analysis for at least two project scenarios using a hypothetical budget and justifies the final decision.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course convenor) Liviu PERNIU	(Last name, First name, signature of seminar/ laboratory/ project convenor) Liviu PERNIU
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

6) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

7) Study level – choose from among: BA/MA/PhD;

8) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

9) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

10) One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

DISCIPLINE SHEET

1. Program Data

1.1 Higher education institution	**Transilvania University of Brașov**
1.2 Faculty	**Electrical Engineering and Computer Science**
1.3 Department	**Electronics & Computers**
1.4 Field of Master's studies1)	**Electronic Engineering, Telecommunications and Information Technology**
1.5 Cycle of studies[2)]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Data about the discipline

2.1 Name of the discipline	**Practice**								
2.2 Course Activity Holder									
2.3 Holder of seminar/laboratory/project activities	**Prof. dr. ing. Titus-Constantin BĂLAN**								
2.4 Year of study		2.5 Semester		2.6 Type of assessment		2.7 Discipline regime	Contents3)	**DS**	
							Obligation3)	**DOB**	

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**10**	of which: 3.2 course	**0**	3.3 Seminar / Laboratory / Project	**0/0/10**
3.4 Total hours in the curriculum	**140**	of which: 3.5 course	**0**	3.6 Seminar/ laboratory/ project	**0/0/140**

Partially assisted activities – 10 hours/week	
Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	0
Additional documentation in the library, on specialized electronic platforms and in the field	0
Preparation of seminars / laboratories / projects, assignments, reports, portfolios and essays	0
Tutoring	0
Examination	0
Other activities.....	40

3.7 Total hours of individual study	40
3.8 Total hours per semester	180
3.9 Number of credits5)	6

4. Preconditions (where applicable)

4.1 Curriculum	• This is not the case
4.2 Competencies	• This is not the case

5. Conditions (where applicable)

5.1 Course Schedule	• This is not the case
5.2 Conducting the seminar/laboratory/project	• University laboratories and activity at economic partners • Conditions according to the internship agreement between the university and partners

6. Specific skills acquired (according to the competence grid in the curriculum)

Professional skills	**C.1 Manage System Security** ***Skills*** **R.I.1.3.** Apply detection techniques for security **C.2 Define security policies** ***Skills*** **R.I.2.2.** Designs and executes a set of written rules and policies that aim to ensure an organization in terms of constraints related to stakeholder behavior, mechanical protection constraints, and constraints related to data access **C.3 Implement risk management in ICT** ***Skills*** **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy **C.6 Protects ICT devices** ***Skills*** **R.I.6.3**. Use tools and methods to maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics, and protection systems such as firewall, antivirus, spam filters. ***Responsibility and autonomy*** **R.I.6.4.** Show initiative and action to update professional knowledge in the field of software and hardware security, maximizing the security of computing devices
Transversal competences	

7. Objectives of the discipline (resulting from the specific competences acquired)

7.1 General objective of the discipline	Guiding students in carrying out applied and research projects completed by participating in conferences, scientific communication sessions or articles published in specialized journals
7.2 Specific objectives	• encouraging students to develop research ideas • engaging students in individual research projects or in partnership with agents from the industrial environment • correct writing of a scientific paper, according to the required templates

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Bibliography			
8.2 Seminar/ laboratory/ project Partially assisted activities	Teaching-learning methods	Number of hours	Observations

	Brainstorming discussions to identify topics of interest. Encouraging teamwork. Presentation of examples from the field of interest.	10 hours per week	

Bibliography

Bibliography

[1]. OPTIM http://www.info-optim.ro/authors_kit.php Conference

[2]. Bulletin of the Transilvania University of Braşov http://webbut.unitbv.ro/bulletin/Series%20I/Instructions.html

9. Corroboration of the contents of the discipline with the expectations of the representatives of the epistemic communities, professional associations and representative employers in the field related to the program

Employers' expectations were identified with an important weight in the direction of developing theoretical and practical research skills and applying general knowledge in modern applications.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final grade
10.4 Course			
10.5 Seminar/ laboratory/ project	Research topic in the field of master's specialization	Final evaluation with the presentation of the results of each paper	10%
	Scientific level/degree of interest for agents in the industrial environment		70%
	Degree of novelty / usefulness		10%
	Clarity, coherence, conciseness of the presentation and Explanation of the functionality Work	Evaluation along the way with presentation of phased results	30%
	Presentation of the paper at a conference, scientific communications session or publication in a specialized journal	Acceptance of the paper for support or publication.	10%

10.6 Minimum Performance Standard

Minimum objectives:

R.I.1.3. Apply detection techniques for security

R.I.2.2. Be able to design and implement a set of written rules and policies that aim to ensure an organisation in terms of constraints related to stakeholder behaviour, mechanical protection constraints and constraints related to data access

R.I.3.3. Analyze and manage security risks and incidents

R.I.3.4. Recommend measures to improve your digital security strategy

R.I.6.3. Use tools and methods that maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics and protection systems such as firewall, antivirus, spam filters **R.I.6.4.** Maximize the security of computing devices

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) BĂLAN Titus Constantin 	(Name, Surname, Signature of seminar/laboratory/project holder) BĂLAN Titus Constantin 
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin 	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

1. Field of study - one of the following options is chosen: Bachelor's degree/ Master's degree/ Doctorate (to be completed according to the Nomenclature of fields and specializations/university study programs in force);
2. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
3. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
4. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);
5. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course	Secure Programming and Application Security

2.2 Course convenor			Conf.dr.ing. Silviu DUMITRESCU					
2.3 Seminar/ laboratory/ project convenor			Conf.dr.ing. Silviu DUMITRESCU					
2.4 Study year		2.5 Semester		2.6 Evaluation type		2.7 Course status	Content[3)]	SC
							Attendance type[4)]	EC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**3**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/1/0**
3.4 Total number of hours in the curriculum	42	out of which: 3.5 lecture	28	3.6 seminar/ laboratory/ project	0/14/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	21
Additional documentation in libraries, specialized electronic platforms, and field research	25
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	19
Tutorial	9
Examinations	4
Other activities.....	

3.7 Total number of individual study hours	78
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Programming languages, Object Oriented Programming, Software Engineering and Communications
4.2 competences-related	• C3.3 Solving real problems that involves elements of data structures and algorithms, programming and use of microprocessor or microcontrollers • C3.4 Programming in a general and / or specific programming language starting from specification, debugging and interpretation of results in correlation with the processor used

5. Conditions (if applicable)

5.1 for course development	• Room equipped with multimedia equipment and white board. Room capacity according with the number of registered students
5.2 for seminar/ laboratory/ project development	• For tutoring at partially assisted hours: laboratory equipped with workstations (computers) for specific experiments and Internet access

6. Specific competences

Professional competences	C2.1. Use of modern acquisition, measurement, compression, transmission and processing techniques, at the basic OSI levels – starting with ensuring the physical support of electronic and communication systems. Definition of the principles and methods of transmission of voice, audio, video and data messages, as well as the principles of integration of services in packet-switched networks C3.1. Mastery of functional modeling techniques of sub-systems, specification of flows and processes, from the application level, in the perspective of use, with an orientation on services and interoperability
Transversal competences	CT3 Objective self-assessment of the need for continuous professional training and openness to lifelong learning and to everything new, as well as the efficient use of language skills, information technology knowledge and communication for personal and professional development, for the purpose of insertion into the labor market and adaptation to the dynamics of its requirements.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	•
7.2 Specific objectives	•

8. Content

8.1 Course	Teaching methods	Number of hours	Remarks
Security relevant C/C++ programming bugs and flaws	Heuristic conversation, Problematization, Case study	2	
Exploitable security flaws	Heuristic conversation, Problematization, Case study	4	
Protection principles	Heuristic conversation, Problematization, Case study	2	
x86 machine code, memory layout, stack operations — Intel 80×86 Processors – main registers — Intel 80×86 Processors – most important instructions — Intel 80×86 Processors – flags — Intel 80×86 Processors – control instructions — Intel 80×86 Processors – stack handling and flow control — The memory address layout — The function calling mechanism in C/C++ on x86 — Calling conventions — The local variables and the stack frame — Function calls – prologue and	Heuristic conversation, Problematization, Case study	2	

epilogue of a function — Stack frame of nested calls — Stack frame of recursive functions			
Buffer Overflow, Stack overflow — Buffer overflow on the stack — Overwriting the return address — Exercise BOFIntro — Exercise BOFShellcode o Protection against stack overflow — Stack overflow – Prevention (during development) — Stack overflow – Detection (during execution) o Stack smashing protection — Stack smashing protection variants — Stack smashing protection in GCC — Exercise BOFShellcode – Stack smashing protection — Effects of stack smashing protection — Bypassing stack smashing protection – an example — Stack overflow – Anti-exploit techniques o Address Space Layout Randomization (ASLR) — Stack randomization with ASLR — Using ASLR — Circumventing ASLR: NOP sledding — Exercise BOFASLR – Circumventing ASLR with NOP sledging o Non executable memory areas – the NX bit — Protection through Virtual Memory Management — Access Control on memory segments — The Never eXecute (NX) bit — Exercise BOFShellcode – Enforcing NX memory segments o Return-to-libc attack – Circumventing the NX bit — Arc injection / Return-to-libc attack — Exercise BOFShellcode – The Return-to-libc attack — Multiple function calls with return-to-libc o Return oriented programming (ROP) — Exploiting with ROP — ROP gadgets — Combining the ROP gadgets — Exercise BOFROP	Heuristic conversation, Problematization, Case study	2	
Heap overflow — Memory allocation managed by a doubly-linked list — Buffer overflow on the heap — Steps of freein g and joining memory blocks — Freeing allocated memory blocks — TLS Heartbeat Extension — Heartbleed – a simple explanation — Heartbleed – fix in v1.0.1g — Protection against heap overflow	Heuristic conversation, Problematization, Case study	2	

Common Coding Errors & Vulnerabilities Input validation — Input validation concepts — Integer problems — Representation of negative integers — Integer ranges — Integer representation by using the two's complement — The integer promotion rule in C/C++ — Arithmetic overflow – spot the bug! — Exercise IntOverflow — So why ABS(INT_MIN)==INT_MIN? — Signedness bug – spot the bug! — Widthness integer overflow – spot the bug! — Exercise Board — A case study – Android Stagefright — Stagefright – a quick introduction — Some Stagefright code examples – spot the bugs! — Integer problem mitigation — Avoiding arithmetic overflow – addition — Avoiding arithmetic overflow – multiplication — Dealing with signed/unsigned integer promotion — Safe integer handling in C — The SafeInt class for C++ — Printf format string bug — Printf format strings — Printf format string bug – exploitation — Exercise Printf — Printf format string exploit – overwriting the return address — Mitigation of printf format string problem — Mitigation of Printf format string problem — Some otherinput validation problems — Array indexing – spot the bug! — The Unicode bug — Directory Traversal Vulnerability — Shellshock – basics of using functions in bash — Shellshock – vulnerability in bash — Exercise – Shellshock — Shellshock fix and counterattacks — Exercise – Command override with environment variables o Improper use of security features — Problems related to the use of security features — Insecure randomness — Week PRNGs in C — Stronger PRNGs in C and Linux — Hardware-based RNGs — Password management — Exercise – Google cracking — Password management and storage — Special purpose hash algorithms for password storage — BDKDF2 and bcrypt implementations in C/C++ — Some other typical password management problems	Heuristic conversation, Problematization, Case study	4	

Improper error and exception handling — Typical problems with error and exception handling — Empty catch block — Overly broad catch — Exercise ErrorHandling – spot the bug! Time and state problems — Time and state related problems — Serialization errors (TOCTTOU) — Attacks with symbolic links — Exercise TOCTTOU o Code quality problems — Dangers arising from poor code quality — Poor code quality – spot the bug! — Unreleased resources — Type mismatch – Spot the bug! — Exercise TypeMismatch			
Advice and Principles of robust programming Matt Bishop's principles of robust programming The security principles of Saltzer and Schroeder	Heuristic conversation, Problematization, Case study	6	
Principles of Secure Web Applications OWASP - Open Web Application Security Project	Heuristic conversation, Problematization, Case study	4	

Bibliography

1. B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007.
2. M. Dowd, J. McDonald and J. Schuh. The Art of Software Security Assessment. Addison-Wesley 2007.
3. David Basin, Patrick Schaller, Michael Schlapfer. Applied Information Security: A Hands-on Approach. Springer, 2011.
4. Fred Long et al. The CERT Oracle Secure Coding Standard for Java, Addison-Wesley, 2012.

8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Remarks
1. Unix Permissions & Tools and GDB Debugger.	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
2. Memory Allocation & Simple Buffer Overflow.	Demonstration, Experiment, Direct actions, Problematization, Case study	2	

3. Stack overflows, corrupting memory & data. Corrupting a network protocol (Java).	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
4. A more advanced buffer overflow. Simple SQL injection. More advanced SQL injection	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
5. A real-life data handling flaw in a version of OpenSSL.	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
6. Web Security. The dynamic linker.	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
7. Cross-site Scripting Attack & Cross-site Request Forgery Attack Lab	Demonstration, Experiment, Direct actions, Problematization, Case study	2	

Bibliography

1. B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007.
2. M. Dowd, J. McDonald and J. Schuh. The Art of Software Security Assessment. Addison-Wesley 2007.
3. David Basin, Patrick Schaller, Michael Schlapfer. Applied Information Security: A Hands-on Approach. Springer, 2011.
4. Fred Long et al. The CERT Oracle Secure Coding Standard for Java, Addison-Wesley, 2012.

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade

10.4 Course	1. The ability to recognize the requirements and to correctly solve applicative problems based on formulas and procedures. 2. The ability to apply the accumulated knowledge to approach new situations, to carry out analyses and comparisons 3. Clarity, consistency, brevity of exposure and functional explanation.	Written examination The scoring scale is explicit and is passed-on to the students with the given subjects	40%
	1. The ability to recognize the requirements and to correctly solve applicative problems based on formulas and procedures. 2. The ability to apply the accumulated knowledge to approach new situations, to carry out analyses and comparisons 3. Clarity, consistency, brevity of exposure and functional explanation.	Half-semester written examination The scoring scale is explicit and is passed-on to the students with the given subjects	10%
10.5 Seminar/ laboratory/ project	Degree of involvement in the practical activity; Attitude towards the practical activity. Participation in debates; Innitiative; Attitudes relative to the matter, teachers and colleagues.	Direct observation. Directioned questioning. Formative evaluation, on the way.	10%
	The capacity to understand the requirements; Ability to resolve the requirements independently;	The colloquium consists in presenting the practical results, and analyzing the implementation. The scoring scale is explicit and is passed-on to the students with the given requirements	40%
10.6 Minimal performance standard			
• R.Î.2.1. Defines data access norms and policies • R.Î.3.1. Identifies possibilities for reducing cybersecurity risks • R.Î.3.2. Develops and implements procedures for identifying, assessing, treating and mitigating ICT risks, such as unauthorized access or data leaks, in accordance with the company's risk strategy, procedures and policies • R.Î.6.2. Protects ICT devices and digital content and understands the risks and threats in digital environments • R.Î.8.4. Shows a spirit of initiative and action to update professional knowledge in the field of software security by saving data in the cloud, with economic and organizational culture aspects.			

This course outline was certified in the Department Board meeting on 25/05/2018 and approved in the Faculty Board meeting on 31/05/2018

(Last name, First name, signature of dean)	(Last name, First name, signature of head of department)
BĂLAN Titus Constantin	STANCA Aurel Cornel
	
Course holder	Holder of seminar/ laboratory/ project
Conf.dr.ing. Silviu DUMITRESCU	Conf.dr.ing. Silviu DUMITRESCU

Note:

11) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

12) Study level – choose from among: BA/MA/PhD;

13) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

14) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

15) One credit is the equivalent of 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course	Secure Web and Internet Technologies
2.2 Course convenor	Conf.dr. Silviu DUMITRESCU
2.3 Seminar/ laboratory/ project convenor	Drd. Vlad FERNOAGĂ

							Content[3)]	SC

2.4 Study year		2.5 Semester		2.6 Evaluation type		2.7 Course status	Attendance type[4)]	EC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**3**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/1/0**
3.4 Total number of hours in the curriculum	42	out of which: 3.5 lecture	28	3.6 seminar/ laboratory/ project	0/14/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	21
Additional documentation in libraries, specialized electronic platforms, and field research	21
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	10
Tutorial	8
Examinations	4
Other activities.....	

3.7 Total number of individual study hours	64
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Programming languages, Object Oriented Programming, Software Engineering and Communications
4.2 competences-related	• C3.3 Solving real problems that involves elements of data structures and algorithms, programming and use of microprocessor or microcontrollers • C3.4 Programming in a general and / or specific programming language starting from specification, debugging and interpretation of results in correlation with the processor used

5. Conditions (if applicable)

5.1 for course development	• Room equipped with multimedia equipment and white board. Room capacity according with the number of registered students
5.2 for seminar/ laboratory/ project development	• For tutoring at partially assisted hours: laboratory equipped with workstations (computers) for specific experiments and Internet access

6. Specific competences

Professional competences	C2.1. Use of modern acquisition, measurement, compression, transmission and processing techniques, at the basic OSI levels – starting with ensuring the physical support of electronic and communication systems. Definition of the principles and methods of transmission of voice, audio, video and data messages, as well as the principles of integration of services in packet-switched networks C3.1. Mastery of functional modeling techniques of sub-systems, specification of flows and processes, from the application level, in the perspective of use, with an orientation on services and interoperability
Transversal competences	CT3 Objective self-assessment of the need for continuous professional training and openness to lifelong learning and to everything new, as well as the efficient use of language skills, information technology knowledge and communication for personal and professional development, for the purpose of insertion into the labor market and adaptation to the dynamics of its requirements.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	Students should get used with Web Application Security concept and testing of security elements on web applications
7.2 Specific objectives	Secure Web Architecture Authentication topics Principles of Secure Web Applications OWASP - Open Web Application Security Project

8. Content

8.1 Course	Teaching methods	Number of hours	Remarks
Secure Web Architecture - Authentication in a Web Application - Access Control (Authorization) - Localization - Password Encoding	Heuristic conversation, Problematization, Case study	4	
Testing of Secure Web Architecture - Tests with mocks - Test Integration - Reactive method security	Heuristic conversation, Problematization, Case study	6	
Web Application Security - Security Filters - Remember-Me Authentication - Basic and Digest Authentication - Cross Site Request Forgery - Security HTTP Response Headers - Session Management - Anonymous Authentication	Heuristic conversation, Problematization, Case study	8	
Advanced Topics - Domain Object Security (ACLs) - Pre-Authentication Scenarios	Heuristic conversation, Problematization, Case study	6	

- LDAP Authentication - CAS Authentication - OAuth Login - Encryptors - Key Generators - Security Context Support			
Principles of Secure Web Applications OWASP - Open Web Application Security Project	Heuristic conversation, Problematization, Case study	4	
Bibliography 1. B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007. 2. M. Dowd, J. McDonald and J. Schuh. The Art of Software Security Assessment. Addison-Wesley 2007. 3. David Basin, Patrick Schaller, Michael Schlapfer. Applied Information Security: A Hands-on Approach. Springer, 2011. 4. Fred Long et al. The CERT Oracle Secure Coding Standard for Java, Addison-Wesley, 2012.			
8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Remarks
Cross-site Scripting Attack Lab	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
Cross-site Request Forgery Attack Lab	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
Web Tracking Lab	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
SQL Injection Attack Lab	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
Web Authentication Methods and Scenarious	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
Session Management	Demonstration, Experiment, Direct actions, Problematization, Case study	2	
Security HTTP	Demonstration, Experiment, Direct actions,	1	

	Problematization, Case study		
Password Encoding	Demonstration, Experiment, Direct actions, Problematization, Case study	1	

Bibliography

1. B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007.
2. M. Dowd, J. McDonald and J. Schuh. The Art of Software Security Assessment. Addison-Wesley 2007.
3. David Basin, Patrick Schaller, Michael Schlapfer. Applied Information Security: A Hands-on Approach. Springer, 2011.
4. Fred Long et al. The CERT Oracle Secure Coding Standard for Java, Addison-Wesley, 2012.

8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Remarks
Auditing and Securing an Web Application	Demonstration, Experiment, Direct actions, Problematization, Case study	14	

Bibliography

1. B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007.
2. M. Dowd, J. McDonald and J. Schuh. The Art of Software Security Assessment. Addison-Wesley 2007.
3. David Basin, Patrick Schaller, Michael Schlapfer. Applied Information Security: A Hands-on Approach. Springer, 2011.
4. Fred Long et al. The CERT Oracle Secure Coding Standard for Java, Addison-Wesley, 2012.

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

Controlling systems via web interfaces became a normal way of operation, so security of web interfaces and implementations is critical.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	1. The ability to recognize the requirements and to correctly solve applicative problems based on formulas and procedures. 2. The ability to apply the accumulated knowledge to approach new situations, to carry out analyses and comparisons 3. Clarity, consistency, brevity of exposure and functional explanation.	Written examination The scoring scale is explicit and is passed-on to the students with the given subjects	40%

	1. The ability to recognize the requirements and to correctly solve applicative problems based on formulas and procedures. 2. The ability to apply the accumulated knowledge to approach new situations, to carry out analyses and comparisons 3. Clarity, consistency, brevity of exposure and functional explanation.	Half-semester written examination The scoring scale is explicit and is passed-on to the students with the given subjects	10%
10.5 Seminar/ laboratory/ project	Degree of involvement in the practical activity; Attitude towards the practical activity. Participation in debates; Innitiative; Attitudes relative to the matter, teachers and colleagues.	Direct observation. Directioned questioning. Formative evaluation, on the way.	10%
	The capacity to understand the requirements; Ability to resolve the requirements independently;	The colloquium consists in presenting the practical results, and analyzing the implementation. The scoring scale is explicit and is passed-on to the students with the given requirements	40%

10.6 Minimal performance standard

- R.Î.2.1. Defines data access norms and policies
- R.Î.3.1. Identifies possibilities for reducing cybersecurity risks
- R.Î.3.2. Develops and implements procedures for identifying, assessing, treating and mitigating ICT risks, such as unauthorized access or data leaks, in accordance with the company's risk strategy, procedures and policies
- R.Î.6.2. Protects ICT devices and digital content and understands the risks and threats in digital environments
- R.Î.8.4. Shows a spirit of initiative and action to update professional knowledge in the field of software security by saving data in the cloud, with economic and organizational culture aspects.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of dean)

BĂLAN Titus Constantin

(Last name, First name, signature of head of department)

STANCA Aurel Cornel

Course holder	Holder of seminar/ laboratory/ project
Conf.dr. Silviu DUMITRESCU	Drd. Vlad FERNOAGĂ

Note:

16) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

17) Study level – choose from among: BA/MA/PhD;

18) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

19) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

20) One credit is the equivalent of 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course			IT Forensics					
2.2 Course convenor			Horia MODRAN					
2.3 Seminar/ laboratory/ project convenor			Horia MODRAN					
2.4 Study year	1	2.5 Semester	1	2.6 Evaluation type	I	2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**2**	out of which: 3.2 lecture	**1**	3.3 seminar/ laboratory/ project	**0/1/0**
3.4 Total number of hours in the curriculum	28	out of which: 3.5 lecture	14	3.6 seminar/ laboratory/ project	0/14/0
Time allocation					hours

Study of textbooks, course support, bibliography and notes	21
Additional documentation in libraries, specialized electronic platforms, and field research	21
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	14
Tutorial	9
Examinations	4
Other activities.....	

3.7 Total number of individual study hours	69
3.8 Total number per semester	125
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Cryptography Fundamentals, Network Fundamentals, Network Security
4.2 competences-related	**C.4 Conducts ICT audits** **C.8 Manages compliance with IT security standards** **C.9 Performs preservation of digital devices for forensic purposes**

5. Conditions (if applicable)

5.1 for course development	• A classroom with at least 30 seats
5.2 for seminar/ laboratory/ project development	• A video projector • A blackboard or whiteboard • A computer lab with individual workstations

6. Specific competences

Professional competences	**C.4 Conducts ICT audits**; L.R.4.1. Identifies and gathers any critical issues and recommends solutions based on relevant standards and best practices. **C.8 Manages compliance with IT security standards**; L.R.9.3. Demonstrates initiative and takes action to guide the implementation of information-security measures and requirements. **C.9 Performs preservation of digital devices for forensic purposes**; L.R.10.1. Identifies methods to preserve the integrity of devices and the data they store for legal evidence collection and use; L.R.10.2. Designs physical preservation methods for computing devices and data-acquisition procedures so that devices and data remain intact and usable for forensic purposes; L.R.10.3. Exhibits responsible, ethical behavior in accordance with the law when establishing procedures to preserve information and devices for forensic retention.

Transversal competences	CT1 Responsible execution of professional tasks, respecting the moral and ethical values, in conditions of autonomy and professional independence, with practical applicability and responsibility for the activities undertaken, in the perspective of Integrating electronic, computing and communications systems with the environment - social, legislative, administrative and ecological – in the terms of sustainable development.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Providing the answers after a cyber-attack took place
7.2 Specific objectives	• Answering the ”5W” (Who, What, When, Where, Why?) in the case of a cyber attack

8. Content

8.1 Course	Teaching methods	Remarks
1. Introduction in IT Forensics	Course 1h	
2. Data acquisition from storage devices	Course 1h	
3. RAM memory acquisition from all Operating Systems I – Windows	Course 1h	
4. RAM memory acquisition from all Operating Systems II – Linux	Course 1h	
5. RAM memory analysis I a. Analysis of the files Pagefile.sys, Hiberfil.sys, Swapfile.sys b. Extraction of the files c. Extraction of the artefacts	Course 1h	
6. RAM memory analysis II a. Analysis of the connections made by the operating system b. Analysis of the processes extracted from RAM c. Analysis of the code injected in RAM	Course 1h	
7. RAM memory analysis III a. Extracting of the relevant information from registry using the specific plugins b. Automating the analysis process of the RAM	Course 1h	
8. Operating Systems log files analysis I a. Windows Event Logs	Course 1h	
9. Operating Systems log files analysis II a. Linux Logs	Course 1h	
10. Analysis of the forensic artefacts of the Operating Systems I a. Registry analysis b. User analysis c. Network connections analysis	Course 1h	

11. Analysis of the forensic artefacts of the Operating Systems II a. USB devices analysis b. Timeline analysis c. Shadow copy volume analysis	Course 1h	
12. Anti-forensic methods identification techniques I	Course 1h	
13. Anti-forensic methods identification techniques II	Course 1h	
14. Recap	Course 1h	
Bibliography 1. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition; Academic Press, 2011, ISBN 978-0123742676 2. Ligh, M. H., Case, A., Levy, J. & Walters, A., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Wiley, 2014, ISBN 978-1118825099 3. Kent, K., Chevalier, S., Grance, T. & Dang, H., Guide to Computer Forensics and Investigations, 4th Edition; Cengage Learning, 2010, ISBN 978-1423905854		
8.2 Seminar/ laboratory/ project	Teaching-learning methods	Remarks
1. Introduction in IT Forensics	Laboratory 1h	
2. Data acquisition from storage devices	Laboratory 1h	
3. RAM memory acquisition from all Operating Systems I – Windows	Laboratory 1h	
4. RAM memory acquisition from all Operating Systems II – Linux	Laboratory 1h	
5. RAM memory analysis I a. Analysis of the files Pagefile.sys, Hiberfil.sys, Swapfile.sys b. Extraction of the files: shimcache and prefetch c. Extraction of the artefacts using Volatility, Rekall, Redline	Laboratory 1h	
6. RAM memory analysis II a. Analysis of the connections made by the operating system b. Analysis of the processes extracted from RAM c. Analysis of the code injected in RAM	Laboratory 1h	
7. RAM memory analysis III a. Extracting of the relevant informations from registry using the plugins (Hivelist, Hivedump, Printkey, Userassist , Hashdump) b. Automating the analysis process the RAM with the software MemGator i Voldiff	Laboratory 1h	
8. Operating Systems log files analysis I	Laboratory 1h	

a. Windows Event Logs		
9. Operating Systems log files analysis II a. Linux Logs	Laboratory 1h	
10. Analysis of the forensic artefacts of the Operating Systems I a. Registry analysis b. User analysis c. Network connections analysis	Laboratory 1h	
11. Analysis of the forensic artefacts of the Operating Systems II a. USB devices analysis b. Timeline analysis c. Shadow copy volume analysis	Laboratory 1h	
12. Anti-forensic methods identification techniques I	Laboratory 1h	
13. Anti-forensic methods identification techniques II	Laboratory 1h	
14. Recap	Laboratory 1h	

Bibliography

1. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition; Academic Press, 2011, ISBN 978-0123742676
2. Ligh, M. H., Case, A., Levy, J. & Walters, A., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Wiley, 2014, ISBN 978-1118825099
3. Kent, K., Chevalier, S., Grance, T. & Dang, H., Guide to Computer Forensics and Investigations, 4th Edition; Cengage Learning, 2010, ISBN 978-1423905854

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

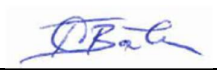
Due to the increase in cyber-attacks, more specialists are needed in this field

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	Clarity and relevance of the answers provided	Exam	40%
		Active attendance	10
10.5 Seminar/ laboratory/ project	Clarity and relevance of the answers provided, activity and participation	Computer assisted evaluation for each laboratory	50%
10.6 Minimal performance standard			

- Examination grade should be at least 5 for both course and laboratory
- **(R.Î.4.1)** Identification and documentation of at least three critical issues in an ICT audit and proposing a basic solution compliant with a recognized standard.
- **(R.Î.9.3)** Drafting and presenting a concise recommendation for implementing an information-security measure, demonstrating initiative in team coordination.
- **(R.Î.10.1)** Description of two methods for preserving the integrity of digital devices and their data.
- **(R.Î.10.2)** Development of a simple guide for the physical preservation of an ICT device and a procedure for data acquisition so that evidence remains unaltered.
- **(R.Î.10.3)** Adherence to a basic ethical code when handling forensic devices and data, demonstrating responsibility throughout all stages of the process.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course holder) Horia MODRAN	(Last name, First name, signature of Holder of seminar/ laboratory/ project) Horia MODRAN ……
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

21) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

22) Study level – choose from among: BA/MA/PhD;

23) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

24) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

25) One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers

1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course			Ethical hacking and security audit					
2.2 Course convenor			Prof. dr. ing. Titus Constantin BĂLAN					
2.3 Seminar/ laboratory/ project convenor			Prof. dr. ing. Titus Constantin BĂLAN					
2.4 Study year	1	2.5 Semester	1	2.6 Evaluation type	I	2.7 Course status	Content[3)]	PC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**4**	out of which: 3.2 lecture	**1**	3.3 seminar/ laboratory/ project	**0/2/1**
3.4 Total number of hours in the curriculum	56	out of which: 3.5 lecture	14	3.6 seminar/ laboratory/ project	0/28/14

Time allocation	hours
Study of textbooks, course support, bibliography and notes	14
Additional documentation in libraries, specialized electronic platforms, and field research	20
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	16
Tutorial	10
Examinations	4
Other activities.....	

3.7 Total number of individual study hours	64
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Computer networks and computer science knowledge, GNU/Linux OS
4.2 competences-related	• **C.3 Implements ICT risk management** • **C.4 Conducts ICT audits** • **C.5 Manages compliance with IT security standards**

5. Conditions (if applicable)

5.1 for course development	• A classroom with at least 30 seats • A video projector

	• A blackboard or whiteboard
5.2 for seminar/ laboratory/ project development	• A computer lab with individual workstations

6. Specific competences

Professional competences	**C.3 Implements ICT risk management**; L.R.3.5. Demonstrates responsible, ethical behavior in accordance with the law when developing procedures to identify cyber threats. **C.4 Conducts ICT audits**; L.R.4.1. Identifies and collects any critical issues and recommends solutions based on applicable standards and best practices**;** L.R.4.2. Organizes and performs audits to evaluate ICT systems, assess the compliance of system components and information-processing systems, and verify information security controls. **C.5 Manages compliance with IT security standards**; L.R.5.2.Ensures the implementation of relevant industry practices, standards, and information-security requirements.
Transversal competences	

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• The formation of skills necessary for managing risks, auditing, and ensuring the compliance of ICT systems with security standards, through the development of ethical and responsible behavior in all stages of the process.
7.2 Specific objectives	• The development of responsible, ethical, and law-abiding behavior for creating and applying procedures to identify cyber threats. • Acquiring the ability to identify and document critical issues within ICT infrastructure and to recommend basic solutions based on recognized standards. • Organizing and conducting an ICT audit to assess the compliance of system components, the functionality of software applications, and the implemented security measures. • The effective implementation, at laboratory or project level, of information security practices, standards, and requirements used in the industry.

8. Content

8.1 Course	Teaching methods	Remarks

1. Introduction	Heuristic dialogue, problematization – 1h	
2. Scanning	Heuristic dialogue, problematization – 2h	
3. System hacking	Heuristic dialogue, problematization – 1h	
4. Trojans	Heuristic dialogue, problematization – 1h	
5. Sniffing the traffic	Heuristic dialogue, problematization – 1h	
6. Denial of Service	Heuristic dialogue, problematization – 1h	
7. Session Hijacking	Heuristic dialogue, problematization – 1h	
8. Web Server Hacking	Heuristic dialogue, problematization – 2h	
9. SQL Injection Attack	Heuristic dialogue, problematization – 2h	
10. Wireless LAN Hacking	Heuristic dialogue, problematization – 1h	
11. Mobile Devices Hacking	Heuristic dialogue, problematization – 1h	

Bibliography

1. Weidman, G., Penetration Testing: A Hands-On Introduction to Hacking, 2nd Edition; No Starch Press, 2017, ISBN 978-1593275648
2. Stuttard, D. & Pinto, M., The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition; Wiley, 2011, ISBN 978-1118026472
3. HackTricks – The Pentesting Notebook, avalabile at https://book.hacktricks.xyz

8.2 Seminar/ laboratory/ project	Teaching-learning methods	Remarks
1. Introduction	Demonstration, Experiment, Direct action, Problematization – 4h	
2. Scanning	Demonstration, Experiment, Direct action, Problematization – 4h	
3. System hacking	Demonstration, Experiment, Direct action, Problematization – 4h	
4. Trojans	Demonstration, Experiment, Direct action, Problematization – 2h	
5. Sniffing the traffic	Demonstration, Experiment, Direct action, Problematization – 4h	

6. Denial of Service	Demonstration, Experiment, Direct action, Problematization – 4h	
7. Session Hijacking	Demonstration, Experiment, Direct action, Problematization – 4h	
8. Web Server Hacking	Demonstration, Experiment, Direct action, Problematization – 6h	
9. SQL Injection Attack	Demonstration, Experiment, Direct action, Problematization – 6h	
10. Wireless LAN Hacking	Demonstration, Experiment, Direct action, Problematization – 2h	
11. Mobile Devices Hacking	Demonstration, Experiment, Direct action, Problematization – 2h	

Bibliography

1. Weidman, G., Penetration Testing: A Hands-On Introduction to Hacking, 2nd Edition; No Starch Press, 2017, ISBN 978-1593275648
2. Stuttard, D. & Pinto, M., The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition; Wiley, 2011, ISBN 978-1118026472
3. HackTricks – The Pentesting Notebook, avalabile at https://book.hacktricks.xyz

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

The knowledge provided by the course is used in the growing field of security audit

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	Clarity and relevance of the answers provided	Exam	40%
		Active attendance	10%
10.5 Seminar/ laboratory/ project	Correct resolution of the exercises. Activity during the laboratories	Evaluation for each laboratory Homework	25%
	Project	Presentation	25%
10.6 Minimal performance standard			
• Examination grade should be at least 5 for both course and laboratory			

• (R.Î.3.5) Applies a simple procedure to identify at least five types of cyber threats in accordance with ethical and legal best practices. • (R.Î.4.1) Identifies and documents at least three critical issues during an ICT audit and proposes a basic solution for each, compliant with a recognized standard. • (R.Î.4.2) Organizes and conducts an introductory ICT audit, evaluating compliance of at least two components and the security of data flows, and delivers a concise report. • (R.Î.5.2) Implements at least one industry-relevant security practice and one standard requirement in a minimal laboratory or project environment.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course convenor) BĂLAN Titus Constantin 	(Last name, First name, signature of seminar/ laboratory/ project convenor) ȘOLCĂ Robert-Nicolae ……
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

26) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

27) Study level – choose from among: BA/MA/PhD;

28) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

29) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

30) One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	***TRANSILVANIA* University of Brasov**
1.2 Faculty	**Electrical Engineering and Computer Science**

1.3 Department	**Electronics and Computers**
1.4 Field of study[1)]	**Engineering in Electronics, Telecommunications and Information Technologies**
1.5 Study level[2)]	**Master**
1.6 Study programme/ Qualification	**Cybersecurity**

2. Data about the course

2.1 Name of course				**Data Processing and Machine Learning Techniques Applied in Cybersecurity**				
2.2 Course convenor				**Ș.l. dr. ing. MODRAN Horia Alexandru**				
2.3 Seminar/ laboratory/ project convenor				**Ș.l. dr. ing. MODRAN Horia Alexandru**				
2.4 Study year	**I**	2.5 Semester	**I**	2.6 Evaluation type		2.7 Course status	Content[3)]	**PC**
							Attendance type[4)]	**CPC**

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**4**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/2/0**
3.4 Total number of hours in the curriculum	**56**	out of which: 3.5 lecture	**28**	3.6 seminar/ laboratory/ project	**0/28/0**
Time allocation					**32**
Study of textbooks, course support, bibliography and notes					**18**
Additional documentation in libraries, specialized electronic platforms, and field research					**30**
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays					**10**
Tutorial					**4**
Examinations					**0**
Other activities.....					**32**

3.7 Total number of individual study hours	**94**
3.8 Total number per semester	**150**
3.9 Number of credits[5)]	**5**

4. Prerequisites (if applicable)

4.1 curriculum-related	Mathematical analysis, Object-oriented programming, Data structures and algorithms
4.2 competences-related	C. 8. Manages compliance with IT security standards

5. Conditions (if applicable)

5.1 for course development	• Lecture class with a minimum of 30 seats, • video projector, • blackboard.

5.2 for seminar/ laboratory/ project development	• Laboratory having computers with Internet connection, Web browser, Python 3 programming environment, Anaconda distribution.

6. Specific competences

Professional competences	C. 1. Manages system security. R. Î. 1.2. Applies detection techniques for security. C. 3. Identifies ICT security risks. R. Î. 3.2. Develops and implements procedures to identify, assess, address and mitigate ICT risks, such as unauthorized access or data leaks, in accordance with the company's risk strategy, procedures and policies. C. 6. Protects ICT devices. R. Î. 6.2. Protects ICT devices and digital content and understands the risks and threats in digital environments.
Transversal competences	CT. 11. Solves problems. R. Î. 11.1. Develops strategies for solving problems. R. Î. 11.2. Finds solutions to the problem. R. Î. 11.3. Apply various strategies for solving problems.

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	Providing an in-depth understanding of Artificial Intelligence (AI) and Machine Learning (ML) technologies, with a focus on their application in the field of Cybersecurity, to identify, prevent and respond to cyber threats.
7.2 Specific objectives	• Develop data preprocessing and analysis skills, including data collection, cleaning, and transformation. • Implement and evaluate ML algorithms using relevant software and tools. • Apply ML algorithms in cybersecurity to detect anomalies, analyse threats, and improve defence systems.

8. Content

8.1 Course	Teaching methods	Number of hours	Remarks
1. Introduction to Data Mining	Interactive course with teaching materials presented with a video projector and running of practical examples	2 hours	
2. Introduction to Machine Learning		2 hours	
3. Supervised Learning: Regression and Classification		2 hours	
4. Unsupervised Learning: Clustering and Dimensionality Reduction		2 hours	
5. Anomaly Detection and Security Applications		2 hours	
6. Fundamentals of Artificial Neural Networks		2 hours	
7. Convolutional Neural Networks and Applications		2 hours	
8. Recurrent Neural Networks and Natural Language Processing		2 hours	

9. Security of Artificial Intelligence (AI) Systems: Challenges and Solutions		2 hours	
10. Adversarial Attacks and Data Poisoning		2 hours	
11. AI in Intrusion Detection and Malware		2 hours	
12. ML Techniques in Vulnerability Analysis		2 hours	
13. AI in Forensics and Incident Response		2 hours	
14. Cybersecurity and Data Privacy Used in AI		2 hours	

Bibliography

1. R. Brown, S. J. Roberts (2023): "Intelligence-Driven Incident Response: Outwitting the Adversary", 2nd Edition, O'Reilly Media, ISBN 978-1098120689.

2. V. Lobo, A. Correia (2022): "Applications of Machine Learning and Deep Learning for Privacy and Cybersecurity", IGI Global, ISBN 978-1799894308.

3. S. Mongeau, A. Hajdasinski (2021): "Cybersecurity Data Science: Best Practices in an Emerging Profession", 1st Edition, Springer, ISBN 978-3030748951.

4. E. Tsukerman (2019): "Machine Learning for Cybersecurity Cookbook", Packt Publishing, ISBN 978-1789614671.

5. C. Chio, D. Freeman (2018): "Machine Learning and Security: Protecting Systems with Data and Algorithm", O'Reilly Media, ISBN 978-1491979907.

6. I. Goodfellow, Y. Bengio, A. Courville (2016): "Deep Learning", MIT Press, ISBN 978-0262035613.

8.2 Laboratory	Teaching-learning methods	Number of hours	Remarks
1. Data Exploration and Preprocessing	Demonstration, Experiment, Direct action, Problematization	2 hours	
2. Implementing Linear and Logistic Regression		2 hours	
3. Applying Clustering Algorithms (K-means, DBSCAN)		2 hours	
4. Dimensionality Reduction with PCA and t-SNE		2 hours	
5. Anomaly Detection with Isolation Forest and SVM		2 hours	
6. Building and Training a Feedforward Neural Network		2 hours	
7. Image Classification with Convolutional Neural Networks		2 hours	
8. Text Generation with Recurrent Neural Networks (LSTM) for Phishing and Deepfake Detection		2 hours	
9. Assessing and Mitigating Adversarial Attacks		2 hours	
10. Implementing Data Poisoning and Prevention Techniques		2 hours	
11. Developing an Intrusion Detection System Based on Machine Learning (ML)		2 hours	
12. Using ML for Vulnerability Analysis		2 hours	
13. Applying ML in Security Incident Investigation		2 hours	
14. Data Privacy and Cybersecurity in AI – Medical Imaging Case Study		2 hours	

Bibliography

1. C. Givre (2024): "Applied Data Science for Cybersecurity", John Wiley & Sons Inc., ISBN 1394244185.

2. A. Géron (2022): " Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems 3rd Edition", 3rd Edition, O'Reilly Media, ISBN 978-1098125974.

3. V. Costa-Gazcón (2021): “Practical Threat Intelligence and Data-Driven Threat Hunting: A hands-on guide to threat hunting with the ATT&CK(TM) Framework and open source tools”, Packt Publishing, ISBN 978-1838556372.

4. F. Chollet (2021): "Deep Learning with Python, Second Edition”, Manning, ISBN 978-1617296864.

5. S. Halder, S. Ozdemir (2018): "Hands-On Machine Learning for Cybersecurity with Python", Packt Publishing, ISBN 978-1788992282.

6. C. Chio, D. Freeman (2018): "Machine Learning & Security: Protecting Systems with Data and Algorithms", O'Reilly Media, ISBN 978-1491979907.

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

The course and lab curriculum reflects the latest trends and challenges in the field, as well as the skills and knowledge required for a successful career in cybersecurity.

The emphasis on Artificial Intelligence and Machine Learning directly responds to the growing need for specialists capable of using these technologies to detect and prevent complex cyber threats. Employers are looking for professionals who can apply machine learning algorithms to analyse large volumes of data, identify patterns, and anticipate attacks. The inclusion of case studies and practical examples ensures that students acquire practical and relevant skills for the job market.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	Knowledge of concepts. Understanding algorithms.	Written exam (The grading scale is explicit and is made known from the beginning of the semester).	45%
	Class activity	Continuous evaluation (assignments / in-class tests)	10%
10.5 Seminar/ laboratory/ project	Evaluation of practical knowledge obtained through participation in laboratory classes.	Practical exam.	45%

10.6 Minimal performance standard

Minimal objectives:

(R. Î. 1.2) For a security event logging dataset, the student will implement and demonstrate the operation of at least one threat detection technique.

(R. Î. 3.2) Starting from a hypothetical network scenario, the student will develop and present a brief report containing the procedure for identifying, assessing, treating and mitigating ICT risks.

(R. Î. 6.2) On a virtual device (virtual machine/container), the student will configure security policies and demonstrate their application through a basic penetration test, highlighting at least one implemented countermeasure.

(R. Î. 11.1) For a hypothetical security incident, the student will develop a documented problem-solving strategy, including its steps and validation criteria.

(R. Î. 11.2) Starting from a practical laboratory exercise, the student will identify and justify an optimal solution to the presented problem, providing rationale for the choice of tools and methodology.

(R. Î. 11.3) Within the scope of a project assignment, the student will apply at least one AI/ML strategy to a given dataset and will analyze its efficiency and accuracy.

This course outline was certified in the Department Board meeting on 25.09.2025 and approved in the Faculty Board meeting on 29.09.2025.

Conf. dr. ing. BĂLAN Titus Constantin,  **Dean**	Ș.l. dr. ing. STANCA Aurel Cornel,  **Head of Department**
Ș.l. dr. ing. MODRAN Horia Alexandru,  **Course holder**	Ș.l. dr. ing. MODRAN Horia Alexandru,  **Laboratory holder**

Note:

31) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

32) Study level – choose from among: BA/MA/PhD;

33) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

34) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

35) One credit is the equivalent of 30 study hours (teaching activities and individual study).

DISCIPLINE SHEET

1. Program Data

1.1 Higher education institution	**Transilvania University of Brașov**
1.2 Faculty	**Electrical Engineering and Computer Science**
1.3 Department	**Electronics & Computers**
1.4 Field of Master's studies1)	**Electronic Engineering, Telecommunications and Information Technology**
1.5 Cycle of studies[2)]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Data about the discipline

2.1 Name of the discipline	**Practice**								
2.2 Course Activity Holder									
2.3 Holder of seminar/laboratory/project activities	**Head of work. Dr. Ing. Dan-Nicolae ROBU**								
2.4 Year of study		2.5 Semester		2.6 Type of assessment		2.7 Discipline regime	Contents3)	**DS**
							Obligation3)	**DOB**

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**10**	of which: 3.2 course	**0**	3.3 Seminar / Laboratory / Project	**0/0/10**
3.4 Total hours in the curriculum	**140**	of which: 3.5 course	**0**	3.6 Seminar/ laboratory/ project	**0/0/140**
Partially assisted activities – 10 hours/week					

Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	0
Additional documentation in the library, on specialized electronic platforms and in the field	0
Preparation of seminars / laboratories / projects, assignments, reports, portfolios and essays	0
Tutoring	0
Examination	0
Other activities.....	40

3.7 Total hours of individual study	40
3.8 Total hours per semester	180
3.9 Number of credits5)	6

4. Preconditions (where applicable)

4.1 Curriculum	• This is not the case
4.2 Competencies	• This is not the case

5. Conditions (where applicable)

5.1 Course Schedule	• This is not the case
5.2 Conducting the seminar/laboratory/project	• University laboratories and activity at economic partners • Conditions according to the internship agreement between the university and partners

6. Specific skills acquired (according to the competence grid in the curriculum)

Professional skills	**C.3 Implement risk management in ICT** ***Skills*** **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy **C.6 Protects ICT devices** ***Responsibility and autonomy*** **R.I.6.4.** Show initiative and action to update professional knowledge in the field of software and hardware security, maximizing the security of computing devices **C.8 Manage compliance with IT security standards** ***Responsibility and autonomy*** **R.I. 8.3** Shows initiative and action to guide the implementation of information security measures and requirements.

Transversal competences	

7. Objectives of the discipline (resulting from the specific competences acquired)

7.1 General objective of the discipline	Guiding students in carrying out applied and research projects completed by participating in conferences, scientific communication sessions or articles published in specialized journals
7.2 Specific objectives	• encouraging students to develop research ideas • engaging students in individual research projects or in partnership with agents from the industrial environment • correct writing of a scientific paper, according to the required templates

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Bibliography			
8.2 Seminar/ laboratory/ project Partially assisted activities	Teaching-learning methods	Number of hours	Observations
	Brainstorming discussions to identify topics of interest. Encouraging teamwork. Presentation of examples from the field of interest.	10 hours per week	
Bibliography [1]. OPTIM http://www.info-optim.ro/authors_kit.php Conference [2]. Bulletin of the Transilvania University of Braşov http://webbut.unitbv.ro/bulletin/Series%20I/Instructions.html			

9. Corroboration of the contents of the discipline with the expectations of the representatives of the epistemic communities, professional associations and representative employers in the field related to the program

The expectations of employers were identified with an important weight in the direction of developing theoretical and practical research skills and applying general knowledge in modern applications.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final grade
10.4 Course			
10.5 Seminar/ laboratory/ project	Research topic in the field of master's specialization	Final evaluation with the presentation of the results of each paper	10%
	Scientific level/degree of interest for agents in the industrial environment		40%

	Degree of novelty / usefulness		10%
	Clarity, coherence, conciseness of the presentation and Explanation of the functionality Work	Evaluation along the way with presentation of phased results	30%
	Presentation of the paper at a conference, scientific communications session or publication in a specialized journal	Acceptance of the paper for support or publication.	10%

10.6 Minimum Performance Standard

Minimum objectives:

R.I.3.3. Analyze and manage security risks and incidents

R.I.3.4. Recommend measures to improve your digital security strategy

R.I.6.4. Maximize the security of computing devices

R.I.8.3. Show initiative and action to guide the implementation of information security measures and requirements

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) Dan-Nicolae ROBU	(Name, Surname, Signature of seminar/ laboratory holder/ Dan-Nicolae ROBU
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin 	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

6. Field of study - one of the following options is chosen: Bachelor's degree/ Master's degree/ Doctorate (to be completed according to the Nomenclature of fields and specializations/university study programs in force);
7. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
8. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
9. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);
10. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course			Malware analysis					
2.2 Course convenor			Alexandru CHIȘ					
2.3 Seminar/ laboratory/ project convenor			Alexandru CHIȘ					
2.4 Study year	1	2.5 Semester	1	2.6 Evaluation type	I	2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**3**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/0/1**
3.4 Total number of hours in the curriculum	42	out of which: 3.5 lecture	28	3.6 seminar/ laboratory/ project	0/0/14

Time allocation	hours
Study of textbooks, course support, bibliography and notes	22
Additional documentation in libraries, specialized electronic platforms, and field research	20
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	20
Tutorial	14
Examinations	2
Other activities.....	

3.7 Total number of individual study hours	78
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Computer science and computer networking knowledge • Cryptography
4.2 competences-related	• C.4 Conducts ICT audits • C.6 Protects ICT devices • C.9 Performs preservation of digital devices for forensic purposes

5. Conditions (if applicable)

5.1 for course development	• Room equipped with multimedia equipment and white board. Room capacity according with the number of registered students
5.2 for seminar/ laboratory/ project development	• Laboratory equipped with workstations (computers) for specific experiments and Internet access

6. Specific competences

Professional competences	**C.4 Conducts ICT audits;** L.R.4.1. Identifies and documents any critical issues found during an ICT audit and recommends solutions based on relevant standards and best practices; L.R.4.2. Organizes and performs audits to evaluate ICT systems, assess the compliance of system components and information-processing systems, and verify information security controls. **C.6 Protects ICT devices;** L.R.6.3. Uses tools and methods to maximize the security of devices and ICT information through access controls, such as strong passwords, digital signatures, biometrics, and protection mechanisms like firewalls, antivirus software, and spam filters. **C.9 Performs preservation of digital devices for forensic purposes;** L.R.10.2. Designs physical preservation methods for computing devices and data acquisition procedures so that devices and their data remain intact and admissible for forensic investigation.
Transversal competences	

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Development of competencies in auditing, protection, and forensic preservation of ICT devices and systems, through strengthening the ability to identify security issues, apply technical and organizational solutions, and ensure the integrity of digital evidence.
7.2 Specific objectives	• Identify and document critical issues during an ICT audit and formulate remediation recommendations based on international standards. • Organize and conduct a full audit of an information system, assessing the compliance of both hardware and software components as well as the effectiveness of implemented security measures. • Utilize access-control tools and protection mechanisms to maximize the security of ICT devices. • Design and implement physical preservation procedures for computing devices and data acquisition methods so that digital evidence remains intact and admissible for forensic investigations.

8. Content

8.1 Course	Teaching methods	Hours	Remarks
1. Introduction	Heuristic dialogue, Problematization	2	
2. Malware Analysis Techniques – operating systems and filesystems	Heuristic dialogue, Problematization	2	
3. Malware Analysis Techniques – assembly language, PE structure and Windows API	Heuristic dialogue, Problematization	4	
4. Malware Analysis applications	Heuristic dialogue, Problematization	4	
5. Reverse Engineering for executable applications	Heuristic dialogue, Problematization	2	
6. Reverse Engineering - Protection methods used by malware	Heuristic dialogue, Problematization	2	
7. Web file and logs analysis	Heuristic dialogue, Problematization	2	
8. Scripts and documents analysis	Heuristic dialogue, Problematization	2	
9. Memory analysis	Heuristic dialogue, Problematization	2	
10. Debugging protected executables and code injection	Heuristic dialogue, Problematization	2	
11. Traffic Analysis	Heuristic dialogue, Problematization	2	
12. Automation and Hunting	Heuristic dialogue, Problematization	2	

Bibliography

1. Sikorski, M. & Honig, A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012, ISBN 978-1593272906
2. Ligh, M. H., Case, A., Levy, J. & Walters, A., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory
3. Russinovich, M., Solomon, D. & Ionescu, A., Windows Internals, 7th Edition; Microsoft Press, 2017, ISBN 978-0735684188

8.2 Seminar/ laboratory/ project	Teaching methods	Hours	Remarks
1. Reverse Engineering	Demonstration, Experiment, Direct action, Problematization.	2	
2. Web file and logs analysis		2	
3. Scripts and documents analysis		2	
4. Memory analysis		2	
5. Debugging protected executables and code injection		2	
6. Traffic Analysis		2	
7. Automation and Hunting		2	

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

Malware attacks increasingly impact business operations, with new variants constantly emerging, and the course prepares specialists for rapid analysis.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	Clarity and relevance of the answers provided	Exam	40%
		Active attendance	10%
10.5 Seminar/ laboratory/ project	Correct resolution of the exercises.	Evaluation of the activity during the laboratory Homework	50%

10.6 Minimal performance standard

- Examination grade should be at least 5 for both course and laboratory
- **(R.Î.4.1)** Extract at least three core elements from a malware sample (e.g., imports, PE sections, strings).
- **(R.Î.4.2)** Execute a malware sample in an isolated sandbox and collect a minimum of five behavioral indicators (e.g., files created/deleted, registry keys modified, network connections).
- **(R.Î.6.3)** Use a free disassembler (e.g., Ghidra, Radare2) to extract and document three types of artifacts (e.g., API calls, injected code, shellcode).
- **(R.Î.10.2)** Follow ethical procedures for handling malware samples throughout the entire analysis process.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course convenor) Alexandru CHIȘ	(Last name, First name, signature of seminar/ laboratory/ project convenor) Alexandru CHIȘ
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

36) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

37) Study level – choose from among: BA/MA/PhD;

38) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

39) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

40) One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course				Malware analysis				
2.2 Course convenor				Alexandru CHIȘ				
2.3 Seminar/ laboratory/ project convenor				Alexandru CHIȘ				
2.4 Study year		2.5 Semester		2.6 Evaluation type		2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**3**	out of which: 3.2 lecture	**2**	3.3 seminar/ laboratory/ project	**0/0/1**
3.4 Total number of hours in the curriculum	42	out of which: 3.5 lecture	28	3.6 seminar/ laboratory/ project	0/0/14

Time allocation	hours
Study of textbooks, course support, bibliography and notes	22
Additional documentation in libraries, specialized electronic platforms, and field research	20
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	20
Tutorial	14
Examinations	2
Other activities.....	

3.7 Total number of individual study hours	78
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	• Computer science and computer networking knowledge

	• Cryptography
4.2 competences-related	• C.4 Conducts ICT audits • C.6 Protects ICT devices • C.9 Performs preservation of digital devices for forensic purposes

5. Conditions (if applicable)

5.1 for course development	• Room equipped with multimedia equipment and white board. Room capacity according with the number of registered students
5.2 for seminar/ laboratory/ project development	• Laboratory equipped with workstations (computers) for specific experiments and Internet access

6. Specific competences

Professional competences	**C.4 Conducts ICT audits;** L.R.4.1. Identifies and documents any critical issues found during an ICT audit and recommends solutions based on relevant standards and best practices; L.R.4.2. Organizes and performs audits to evaluate ICT systems, assess the compliance of system components and information-processing systems, and verify information security controls. **C.6 Protects ICT devices;** L.R.6.3. Uses tools and methods to maximize the security of devices and ICT information through access controls, such as strong passwords, digital signatures, biometrics, and protection mechanisms like firewalls, antivirus software, and spam filters. **C.9 Performs preservation of digital devices for forensic purposes;** L.R.10.2. Designs physical preservation methods for computing devices and data acquisition procedures so that devices and their data remain intact and admissible for forensic investigation.
Transversal competences	

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Development of competencies in auditing, protection, and forensic preservation of ICT devices and systems, through strengthening the ability to identify security issues, apply technical and organizational solutions, and ensure the integrity of digital evidence.
7.2 Specific objectives	• Identify and document critical issues during an ICT audit and formulate remediation recommendations based on international standards. • Organize and conduct a full audit of an information system, assessing the compliance of both hardware and software components as well as the effectiveness of implemented security measures.

	• Utilize access-control tools and protection mechanisms to maximize the security of ICT devices. • Design and implement physical preservation procedures for computing devices and data acquisition methods so that digital evidence remains intact and admissible for forensic investigations.

8. Content

8.1 Course	Teaching methods	Hours	Remarks
13. Introduction	Heuristic dialogue, Problematization	2	
14. Malware Analysis Techniques – operating systems and filesystems	Heuristic dialogue, Problematization	2	
15. Malware Analysis Techniques – assembly language, PE structure and Windows API	Heuristic dialogue, Problematization	4	
16. Malware Analysis applications	Heuristic dialogue, Problematization	4	
17. Reverse Engineering for executable applications	Heuristic dialogue, Problematization	2	
18. Reverse Engineering - Protection methods used by malware	Heuristic dialogue, Problematization	2	
19. Web file and logs analysis	Heuristic dialogue, Problematization	2	
20. Scripts and documents analysis	Heuristic dialogue, Problematization	2	
21. Memory analysis	Heuristic dialogue, Problematization	2	
22. Debugging protected executables and code injection	Heuristic dialogue, Problematization	2	
23. Traffic Analysis	Heuristic dialogue, Problematization	2	
24. Automation and Hunting	Heuristic dialogue, Problematization	2	
Bibliography 4. Sikorski, M. & Honig, A., Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press, 2012, ISBN 978-1593272906 5. Ligh, M. H., Case, A., Levy, J. & Walters, A., The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory 6. Russinovich, M., Solomon, D. & Ionescu, A., Windows Internals, 7th Edition; Microsoft Press, 2017, ISBN 978-0735684188			
8.2 Seminar/ laboratory/ project	Teaching methods	Hours	Remarks
8. Reverse Engineering	Demonstration, Experiment, Direct action, Problematization.	2	
9. Web file and logs analysis		2	
10. Scripts and documents analysis		2	
11. Memory analysis		2	
12. Debugging protected executables and code injection		2	

13. Traffic Analysis		2	
14. Automation and Hunting		2	

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

Malware attacks increasingly impact business operations, with new variants constantly emerging, and the course prepares specialists for rapid analysis.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	Clarity and relevance of the answers provided	Exam	40%
		Active attendance	10%
10.5 Seminar/ laboratory/ project	Correct resolution of the exercises.	Evaluation of the activity during the laboratory Homework	50%

10.6 Minimal performance standard

- Examination grade should be at least 5 for both course and laboratory
- **(R.Î.4.1)** Extract at least three core elements from a malware sample (e.g., imports, PE sections, strings).
- **(R.Î.4.2)** Execute a malware sample in an isolated sandbox and collect a minimum of five behavioral indicators (e.g., files created/deleted, registry keys modified, network connections).
- **(R.Î.6.3)** Use a free disassembler (e.g., Ghidra, Radare2) to extract and document three types of artifacts (e.g., API calls, injected code, shellcode).
- **(R.Î.10.2)** Follow ethical procedures for handling malware samples throughout the entire analysis process.

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of course convenor) Alexandru CHIȘ	(Last name, First name, signature of seminar/ laboratory/ project convenor) Alexandru CHIȘ
(Last name, First name, signature of dean) BĂLAN Titus Constantin 	(Last name, First name, signature of head of department) STANCA Aurel Cornel

Note:

41) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

42) Study level – choose from among: BA/MA/PhD;

[43] Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

[44] Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

[45] One credit is the equivalent of 25 – 30 study hours (teaching activities and individual study).

DISCIPLINE SHEET

1. Program Data

1.1 Higher education institution	**Transilvania University of Brașov**
1.2 Faculty	**Electrical Engineering and Computer Science**
1.3 Department	**Electronics & Computers**
1.4 Field of Master's studies1)	**Electronic Engineering, Telecommunications and Information Technology**
1.5 Cycle of studies[2)]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Data about the discipline

2.1 Name of the discipline	**Practice for the elaboration of the dissertation paper**							
2.2 Course Activity Holder								
2.3 Holder of seminar/laboratory/project activities	**Head of work. Dr. Ing. Dan-Nicolae ROBU**							
2.4 Year of study		2.5 Semester		2.6 Type of assessment		2.7 Discipline regime	Contents3)	**DS**
							Obligation3)	**DOB**

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**8**	of which: 3.2 course	**0**	3.3 Seminar / Laboratory / Project	**0/0/8**
3.4 Total hours in the curriculum	**112**	of which: 3.5 course	0	3.6 Seminar/ laboratory/ project	**0/0/112**
Partially assisted activities – 8 hours/week;					

Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	0
Additional documentation in the library, on specialized electronic platforms and in the field	0
Preparation of seminars / laboratories / projects, assignments, reports, portfolios and essays	0
Tutoring	0
Examination	0
Other activities.....	188

3.7 Total hours of individual study	188

3.8 Total hours per semester	300
3.9 Number of credits5)	10

4. Preconditions (where applicable)

4.1 Curriculum	• This is not the case
4.2 Competencies	• This is not the case

5. Conditions (where applicable)

5.1 Course Schedule	•
5.2 Conducting the seminar/laboratory/project	• Conditions according to the internship agreement between the university and partners

6. Specific skills acquired (according to the competence grid in the curriculum)

Professional skills	**C.1 Manage System Security** ***Skills*** **R.I.1.4.** Analyzes a company's critical assets and identifies weaknesses and vulnerabilities that led to intrusion or attack **C.2 Define security policies** ***Skills*** **R.I.2.2.** Designs and executes a set of written rules and policies that aim to ensure an organization in terms of constraints related to stakeholder behavior, mechanical protection constraints, and constraints related to data access **C.3 Implement risk management in ICT** ***Skills*** **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy ***Responsibility and autonomy*** **R.I.3.5.** Has a responsible, ethical behavior, in the spirit of the law to carry out procedures for identifying cyber threats **C.4 Carry out ICT audits** ***Knowledge*** **R.I.4.1.** Identifies and collects any critical issues and recommends solutions based on the necessary standards and solutions **C.5 Manage compliance with IT security standards** ***Responsibility and autonomy*** **R.I. 5.3** Shows a spirit of initiative and action to guide the implementation of measures and requirements in the field of information security. **C.6 Protects ICT devices** ***Skills*** **R.I.6.3**. Use tools and methods to maximize the security of ICT devices and information through access control, such as passwords, digital signatures, biometrics, and protection systems such as firewall, antivirus, spam filters. ***Responsibility and autonomy*** **R.I.6.4.** Show initiative and action to update professional knowledge in the field of software and hardware security, maximizing the security of computing devices
Transversal competences	**CT.11 Solve problems** **R.I.11.1**. Develop problem-solving strategies

7. Objectives of the discipline (resulting from the specific competences acquired)

7.1 General objective of the discipline	This discipline is designed as a support for students in the realization of the dissertation work. Students are guided and monitored, in close communication with the supervisors of the dissertation works and the institution where the practice takes place for the elaboration of the final projects both in terms of practical implementation and at the level of documentation and presentation method.
7.2 Specific objectives	The secondary objectives deriving from the main objective are:

	-to develop the capacity for analysis, based on bibliography and web-graphy, in order to frame the project in the world stage - Getting used to the work environment in companies - to have contact with the research environment and specific methods - to develop inventiveness by finding modeling and simulation methods that prepare the practical realization; - testing and exploitation of the proposed solution, comparative interpretation of the results; - laying the foundations for entrepreneurial skills and economic management of projects.

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Bibliography			
8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Observations
	PBL (Project-Based Learning) project-based learning. Students present the current state of research and practical experiment, relative to the topic addressed. Practical ideas/guidance/solutions are provided for problems encountered by students and for further research in their chosen field.	112	
Bibliography For this discipline, the bibliography is recommended by each dissertation project supervisor and is written on the first sheet of the diploma project. The bibliography contains both works of the project supervisor and reference works in the field in which the student has chosen the project theme and it is necessary to achieve the current stage in the chosen field.			

9. Corroboration of the contents of the discipline with the expectations of the representatives of the epistemic communities, professional associations and representative employers in the field related to the program

Employers' expectations were identified with an important weight in the direction of developing theoretical and practical research skills and applying general knowledge in modern applications.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final grade
10.4 Course			
10.5 Seminar/ laboratory/ project	1. Clarity, coherence, conciseness of presentation and explanation of research results	The colloquium consists of the discussion on the written support and the hearing of the presentation	70%

	2. Correctness of the practical experiment 3. Value of use of the project. 4. Rationale and theoretical support supporting the experiment Quality of presentation.	(discussion, answers, questions, analyses) The grade is awarded after the Power Point presentation or the document presenting the status of the dissertation project and the activities carried out within the practice.	
	Ability to achieve the current state Understanding phenomena; 2. The ability to apply the accumulated knowledge; 3. Participation in debates Initiatives	Formative evaluation, along the way: Direct observation, Survey questions, etc.	30%
10.6 Minimum Performance Standard			
The colloquium certifies the formation of the competencies stated and the grade reflects the extent to which the competencies are formed. Minimum knowledge: knowledge of the current state of the field in which the diploma project is carried out, establishing the work plan, establishing the structure of the documentation, supplying components or software, clarifying the practical experiment.			

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) Dan-Nicolae ROBU	(Name, Surname, Signature of seminar/laboratory/project holder) Dan-Nicolae ROBU
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin 	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

11. Field of study - one of the following options is chosen: Bachelor's degree/ Master's degree/ Doctorate (to be completed according to the Nomenclature of fields and specializations/university study programs in force);
12. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
13. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
14. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);

15. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

DISCIPLINE SHEET

1. Program Data

1.1 Higher education institution	**Transilvania University of Braşov**
1.2 Faculty	**Electrical Engineering and Computer Science**
1.3 Department	**Electronics & Computers**
1.4 Field of Master's studies1)	**Electronic Engineering, Telecommunications and Information Technology**
1.5 Cycle of studies[2)]	**Masters**
1.6 Study Programme/ Qualification	**Cybersecurity**

2. Data about the discipline

2.1 Name of the discipline	Elaboration of the dissertation paper							
2.2 Course Activity Holder								
2.3 Holder of seminar/laboratory/project activities	Prof. dr. ing. Titus-Constantin BĂLAN							
2.4 Year of study		2.5 Semester		2.6 Type of assessment		2.7 Discipline regime	Contents3)	DSI
							Obligation3)	DI

3. Total estimated time (hours per semester of teaching activities)

3.1 Number of hours per week	**8**	of which: 3.2 course	**0**	3.3 Seminar / Laboratory / Project	**0/0/8**
3.4 Total hours in the curriculum	112	of which: 3.5 course	0	3.6 Seminar/ laboratory/ project	0/0/112

Partially assisted activities – 2 hours/week; Unassisted activities - 5 hours / week

Time Pool Distribution	Hours
Study by textbook, course material, bibliography and notes	0
Additional documentation in the library, on specialized electronic platforms and in the field	0
Preparation of seminars / laboratories / projects, assignments, reports, portfolios and essays	0
Tutoring	0
Examination	
Other activități.de work at the practice site	188

3.7 Total hours of individual study	188
3.8 Total hours per semester	300
3.9 Number of credits5)	10

4. Preconditions (where applicable)

4.1 Curriculum	• Completion of all courses
4.2 Competencies	• This is not the case

5. Conditions (where applicable)

5.1 Course Schedule	• This is not the case
5.2 Conducting the seminar/laboratory/project	• Conditions according to the internship agreement between the university and partners

6. Specific skills acquired (according to the competence grid in the curriculum)

Professional skills	**C.1 Manage System Security** ***Skills*** **R.I.1.4.** Analyzes a company's critical assets and identifies weaknesses and vulnerabilities that led to intrusion or attack **C.2 Define security policies** ***Skills*** **R.I.2.2.** Designs and executes a set of written rules and policies that aim to ensure an organization in terms of constraints related to stakeholder behavior, mechanical protection constraints, and constraints related to data access **C.3 Implement risk management in ICT** ***Skills*** **R.I.3.2.** Develops and implements procedures for identifying, assessing, dealing with and mitigating ICT risks, such as unauthorised access or data leakage, in accordance with the company's strategy, procedures and risk policies **R.I.3.3.** Analyze and manage security risks and incidents **R.I.3.4.** Recommend measures to improve your digital security strategy ***Responsibility and autonomy*** **R.I.3.5.** Has a responsible, ethical behavior, in the spirit of the law to carry out procedures for identifying cyber threats **C.4 Carry out ICT audits** ***Skills*** **R.I.4.2.** Organises and conducts audits in order to assess ICT systems, compliance of system components, information processing information systems and information security **C.5 Manage compliance with IT security standards** ***Responsibility and autonomy*** **R.I. 5.3** Shows a spirit of initiative and action to guide the implementation of measures and requirements in the field of information security. **C.6 Protects ICT devices** ***Responsibility and autonomy*** **R.I.6.4.** Show initiative and action to update professional knowledge in the field of software and hardware security, maximizing the security of computing devices

Transversal competences	**CT.11 Solve problems** **R.I.11.2.** Find solutions to problems

7. Objectives of the discipline (resulting from the specific competences acquired)

7.1 General objective of the discipline	Analysis, design and simulation of electronics and telecommunications systems This discipline is designed as a support for students in the realization of the dissertation work. Students are guided and monitored, in close communication with the supervisors of the dissertation works and the institution where the practice takes place for the elaboration of the final projects both in terms of practical implementation and at the level of documentation and presentation method.
7.2 Specific objectives	The secondary objectives deriving from the main objective are: -to develop the capacity for analysis, based on bibliography and web-graphy, in order to frame the project in the world stage - Getting used to the work environment in companies - to have contact with the research environment and specific methods - to develop inventiveness by finding modeling and simulation methods that prepare the practical realization; - testing and exploitation of the proposed solution, comparative interpretation of the results; - laying the foundations for entrepreneurial skills and economic management of projects.

8. Contents

8.1 Course	Teaching methods	Number of hours	Observations
Bibliography			
8.2 Seminar/ laboratory/ project	Teaching-learning methods	Number of hours	Observations
	Tutoring activity for guidance in the elaboration of the dissertation work	112	
Bibliography For this discipline, the bibliography is recommended by each dissertation project supervisor and is written on the first sheet of the diploma project. The bibliography contains both works of the project supervisor and reference works in the field in which the student has chosen the project theme and it is necessary to achieve the current stage in the chosen field.			

9. Corroboration of the contents of the discipline with the expectations of the representatives of the epistemic communities, professional associations and representative employers in the field related to the program

Employers' expectations were identified with an important weight in the direction of developing theoretical and practical research skills and applying general knowledge in modern applications.

10. Rating

Type of activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Weight in the final grade
10.4 Course			
10.5 Seminar/ laboratory/ project	1. Clarity, coherence, conciseness of presentation and explanation of research results 2. Correctness of the practical experiment 3. Value of use of the project. 4. Rationale and theoretical support supporting the experiment 5. Quality of presentation.	The colloquium consists of the discussion on the written support and the hearing of the presentation (discussion, answers, questions, analyses) The grade is awarded after the Power Point presentation or the document presenting the status of the dissertation project and the activities carried out within the practice.	70%
	1. Capacity to achieve the current state Understanding phenomena; 2. The ability to apply the accumulated knowledge; 3. Participation in debates Initiatives	Formative evaluation, along the way: Direct observation, Survey questions, etc.	30%
10.6 Minimum Performance Standard			
The colloquium certifies the formation of the competencies stated and the grade reflects the extent to which the competencies are formed. Minimum knowledge: knowledge of the current status of the field in which the diploma project is carried out, establishing the work plan, establishing the structure of the documentation, supplying components or software, clarifying the practical experiment			

This Disciplinary Sheet was endorsed in the meeting of the Department Council on 29/09/2025 and approved in the meeting of the Faculty Council on 29/09/2025.

(Name, Surname, Signature of the course holder) BĂLAN Titus Constantin	(Name, Surname, Signature of seminar/laboratory/project holder) BĂLAN Titus Constantin
(Name, Surname, Dean's Signature) BĂLAN Titus Constantin	(Name, Surname, Signature of the department director) STANCA Aurel Cornel

Note:

16. Field of study - one of the following options is chosen: Bachelor's degree/ Master's degree/ Doctorate (to be completed according to the Nomenclature of fields and specializations/university study programs in force);
17. Cycle of studies - one of the following options is chosen: Bachelor's / Master's / Doctorate;
18. Discipline regime (content) - one of the variants is chosen: DF (fundamental discipline)/ DD (discipline in the field)/ DS (specialized discipline)/ DC (complementary discipline) - for the bachelor's level; DAP (in-depth discipline)/ DSI (synthesis discipline)/ DCA (advanced knowledge discipline) - for the master's level;
19. Discipline regime (compulsory) - one of the following variants is chosen: DI (compulsory subject)/ DO (optional subject)/ DFac (optional subject);
20. One credit is equivalent to 25 – 30 hours of study (teaching activities and individual study).

COURSE OUTLINE

1. Data about the study programme

1.1 Higher education institution	Transilvania University of Brasov
1.2 Faculty	Electrical Engineering and Computer Science
1.3 Department	Electronics and Computers
1.4 Field of study[1)]	Engineering in Electronics, Telecommunications and Information Technologies
1.5 Study level[2)]	MA
1.6 Study programme/ Qualification	Cyber Security

2. Data about the course

2.1 Name of course								
2.2 Course convenor								
2.3 Seminar/ laboratory/ project convenor								
2.4 Study year		2.5 Semester		2.6 Evaluation type		2.7 Course status	Content[3)]	SC
							Attendance type[4)]	CPC

3. Total estimated time (hours of teaching activities per semester)

3.1 Number of hours per week	**2**	out of which: 3.2 lecture	**1**	3.3 seminar/ laboratory/ project	**14/ 0/0**
3.4 Total number of hours in the curriculum	28	out of which: 3.5 lecture	14	3.6 seminar/ laboratory/ project	14/ 0/0

Time allocation	hours
Study of textbooks, course support, bibliography and notes	24
Additional documentation in libraries, specialized electronic platforms, and field research	30
Preparation of seminars/ laboratories/ projects, homework, papers, portfolios, and essays	18
Tutorial	18

Examinations	2
Other activities.....	

3.7 Total number of individual study hours	92
3.8 Total number per semester	120
3.9 Number of credits[5)]	4

4. Prerequisites (if applicable)

4.1 curriculum-related	•
4.2 competences-related	•

5. Conditions (if applicable)

5.1 for course development	• video projector
5.2 for seminar/ laboratory/ project development	• computer network • virtual machines • specialized programs

6. Specific competences

Professional competences	• Developing teamwork skills to develop complex applications
Transversal competences	•

7. Course objectives (resulting from the specific competences to be acquired)

7.1 General course objective	• Developing knowledge and skills of using information and communication technology in the analysis, synthesis and design of cyber security systems.
7.2 Specific objectives	• Formation of attitudes and values needed for constructivist approaches to specific information society issues - design of Enterprise Architecture and Business Performance. Familiarize the future specialist with models, means and design techniques that build on the prototype of software products throughout the lifecycle. Students' teamwork is developed and developed.

8. Content

<table>
<tr><td>8.1 Course</td><td>Teaching methods</td><td>Remarks</td></tr>
<tr><td>Enterprise architecture foundational concepts</td><td rowspan="8">Exercise the use of the index of terms.
The conversation / dialog method.
Using video recordings and presentations.
The conversation / dialog method.</td><td>1</td></tr>
<tr><td>Enterprise architecture methodologies</td><td>2</td></tr>
<tr><td>Data security architecture for organizations</td><td>1</td></tr>
<tr><td>Organizational change management</td><td>2</td></tr>
<tr><td>Strategic planning for organization</td><td>1</td></tr>
<tr><td>Setting strategic directions: roles and responsibilities</td><td>2</td></tr>
<tr><td>Organization performance methodology: Balanced Scorecard</td><td>3</td></tr>
<tr><td>Data collection methods for assessing organization performance</td><td>2</td></tr>
<tr><td colspan="3">Bibliography
• Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology Steven H. Spewak, Wiley 1993;
• Enterprise Architecture As Strategy: Creating a Foundation for Business Execution by Jeanne W. Ross, Peter Weill, David C. Robertson, Harvard Business Press (2006);
• Federal Enterprise Architecture Framework , version 2, January 2013;
• Balanced Scorecard: Step-by-Step for Government and Nonprofit Agencies 2nd Edition, Paul NIVEN, 2015
• The Balanced Scorecard: Translating Strategy into Action Hardcover, Roberst S. Kaplan, 1996</td></tr>
<tr><td>8.2 Seminar/ laboratory/ project</td><td>Teaching-learning methods</td><td>Remarks</td></tr>
<tr><td>Enterprise architecture foundational concepts</td><td rowspan="8">Conversation,
Demonstration,
Case studies,
Evaluation.</td><td>1</td></tr>
<tr><td>Enterprise architecture methodologies, FEAF Example</td><td>2</td></tr>
<tr><td>Building diagram relations</td><td>1</td></tr>
<tr><td>Develop a change management plan</td><td>1</td></tr>
<tr><td>Organization performance concepts</td><td>2</td></tr>
<tr><td>Develop strategic directions</td><td>1</td></tr>
<tr><td>Using balance scorecard methodology</td><td>4</td></tr>
<tr><td>Establish and measure performance indicators</td><td>2</td></tr>
<tr><td colspan="3">Bibliography
• Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology Steven H. Spewak, Wiley 1993;
• Enterprise Architecture As Strategy: Creating a Foundation for Business Execution by Jeanne W. Ross, Peter Weill, David C. Robertson, Harvard Business Press (2006);
• Federal Enterprise Architecture Framework , version 2, January 2013;
• Balanced Scorecard: Step-by-Step for Government and Nonprofit Agencies 2nd Edition, Paul NIVEN, 2015;
• The Balanced Scorecard: Translating Strategy into Action Hardcover, Robert S. Kaplan, 1996;
• Creating Strategic Models with Enterprise Architect, Sparx Systems & Stephen Maguire, 2017.</td></tr>
</table>

9. Correlation of course content with the demands of the labour market (epistemic communities, professional associations, potential employers in the field of study)

The content of the discipline belongs to the field of applied informatics and is meant for information and communication technology in the analysis, synthesis and evaluation of data. Data handling is applicable to any field of activity that uses electronic means of operation.

10. Evaluation

Activity type	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of the final grade
10.4 Course	The quality of the evaluation achieved by analyzing, synthesizing, generalizing the data obtained through its own investigation	Summative assessment (written exam evaluation method) - traditional theoretical knowledge test	60%
	Quality of judgments, logical thinking, flexibility	Formal evaluation - assessment during laboratory performance (at the end of each laboratory). Project development	30%
10.5 Seminar/ laboratory/ project	Quality of judgments, logical thinking, flexibility	Summative assessment - assessment by practice - on the computer. Final test	10%
10.6 Minimal performance standard			
• The final exam average is calculated only if the grade obtained in the theoretical test and the grade obtained at the practical test (according to the scales initially announced) are at least 5. • R.Î.4.3.Performs processes in the management of cybersecurity projects, taking on different roles in the team and describing clearly and concisely, verbally and in writing, the results • R.Î.11.3. Performs processes in the management of cybersecurity projects, taking on different roles in the team and describing clearly and concisely, verbally and in writing, the results. • R.Î.13.1. Analyzes business processes starting from the cost/benefit ratio of a project starting from the budget of a profile company or of an own enterprise • R.Î.13.2. Determines the contribution of work processes to commercial objectives and plans the allocation of resources and investment and operational measures of high productivity			

This course outline was certified in the Department Board meeting on 29/09/2025 and approved in the Faculty Board meeting on 29/09/2025

(Last name, First name, signature of dean)	(Last name, First name, signature of head of department)
BĂLAN Titus Constantin	STANCA Aurel Cornel
	
Course holder	Holder of seminar/ laboratory/ project
Prof.dr.ing. Sorin-Aurel MORARU	Drd Florin OGIGAU-NEAMȚIU

Note:

46) Field of study – select one of the following options: BA/MA/PhD. (to be filled in according to the forceful classification list for study programmes);

47) Study level – choose from among: BA/MA/PhD;

48) Course status (content) – for the BA level, select one of the following options: FC (fundamental course) / DC (course in the study domain)/ SC (speciality course)/ CC (complementary course); for the MA level, select one of the following options: PC (proficiency course)/ SC (synthesis course)/ AC (advanced course);

49) Course status (attendance type) – select one of the following options: CPC (compulsory course)/ EC (elective course)/ NCPC (non-compulsory course);

50) One credit is the equivalent of 30 study hours (teaching activities and individual study).