SYLLABUS

INFORMATION SYSTEM SECURITY

1. **Information on academic programme**

1.1. University	**„1 Decembrie 1918" University of Alba Iulia**
1.2. Faculty	**Faculty of Informatics and Engneering**
1.3. Department	**Informatics, Mathematics and Electronics Department**
1.4. Field of Study	**Computer Science**
1.5. Cycle of Study	**Undergraduate**
1.6. Academic programme / Qualification	**Computer Science**

2. **Information of Course Matter**

2.1. **Course**		*Information system security*				2.2. **Code**	CSE 315
2.3. **Course Leader**			Lect. Phd. Incze Arpad				
2.4. **Seminar Tutor**			Lect. Phd. Incze Arpad				
2.5. Academic Year	**III**	2.6. Semester	**II**	2.7. Type of Evaluation (E – final exam/ CE - colloquy examination / CA -continuous assessment)	**E**	2.8. Type of course (**C**– Compulsory, **Op** – optional, **F** - Facultative)	**O**

3. Course Structure (Weekly number of hours)

3.1. Weekly number of hours	**4**	3.2. course	***2***	3.3. seminar, laboratory	***2***
3.4. Total number of hours in the curriculum	**56**	3.5. course	***28***	3.6. seminar, laboratory	***28***

Allocation of time:	Hours
Individual study of readers	***40***
Documentation (library)	***20***
Home assignments, Essays, Portfolios	***28***
Tutorials	**-**
Assessment (examinations)	***6***
Other activities…….	**-**

3.7 Total number of hours for individual study	**94**
3.9 Total number of hours per semester	**150**
3.10 Number of ECTS	**6**

4. Prerequisites (*where applicable*)

4.1. curriculum-based	***Compulsory prerequisites*** CSE 110 Operating systems CSE 203 Computer networks CSE 211 WEB applications development
4.2. competence-based	

5.Requisites (*where applicable*)

5.1. course-related	*The course is hosted in a room equipped with video projector* ***Note:*** *The students are strongly encouraged to attend the course, in order to gain knowledge for practical applications.*
5.2. seminar/laboratory-based	*The seminar is hosted in a laboratory equipped with video projector and computers* ***Note:*** *The attendance of the laboratory classes is compulsory.*

6. Specific competences to be acquired (chosen by the course leader from the program general competences grid)

Professional competences	C6 Network Design and Administration C6.1. Identification of basic concepts and models computer systems and computer networks C6.3. Use of acquired techniques for installing configuring and maintaining computer systems and networks C6.4. Performance measurements and access rights
Transversal competences	-

7. Course objectives (as per the programme specific competences grid)

7.1 General objectives of the course	Acquiring the fundamental knowledge about concepts, mechanisms, problemes and tools in conjunction with computer system/network security
7.2 Specific objectives of the course	Understanding the security related side of design and implementation of computer systems Understanding of attacks on security and prevention and defence mechanism and tools to prevent or defend those attacks Learning the mechanism methods and techniques of secure programming

8. Course contents

8.1 Course (learning units)	**Teaching methods**	**Remarks**
1. Security issues and principles	***Lecture, discussion***	
2. Security of operating systems . Access control	***Lecture, discussion***	
3. Network security.Vulnerabilities, Attacks types	***Lecture, discussion***	
4. Wireless network security	***Lecture, discussion***	
5. Network security. Firewalls and IDS	***Lecture, discussion***	
6. Virus and malware	***Lecture, discussion***	
7. Software security. Defensive programming	***Lecture, discussion***	
8. Web application security	***Lecture, discussion***	
9. Penetration testing techniques	***Lecture, discussion***	
10. Security auditing and security policies	***Lecture, discussion***	
11. Introduction to cryptography. History and basics. Symmetric and Asymmetric cryptography	***Lecture, discussion***	
12. Key distribution and authentication protocols	***Lecture, discussion***	

Reference:

1. Dieter Gollmann. *Computer Security*. ed. 3, Wiley, 2011
2. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 2001
3. Ross J. Anderson. *Security Engineering*. ed. 2, Wiley, 2008
4. M. Down, J. McDonald, J. Schuh, „ The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities ”, AddisonWesley, 2007
5. M. Howard, D. LeBlanc, J. Viega, „ 24 Deadly Sins of Software Security. Programming Flows and How to Fix Them ”, McGraw Hill, 2010

6. M. Howard, D. LeBlanc, „ Writing Secure Code for Windows Vista ”, Microsoft Press, 2007
7. G. McGraw, „ Software Security:Building Security In ”, AddisonWesley, 2006
8. R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems”, AddisonWesley, 2 nd edition, 2014
9. , „ Common Weaknesses Enumeration (WCE)”, online: http://cwe.mitre.org/data/index.html

Seminars-laboratories	**Teaching methods**	
User access rights in windows and linux	***Coordination and evaluation of computer-based works***	-
File access control in Windows and Linux. File execution privileges	***Coordination and evaluation of computer based works***	-
Network security. Router and switch configurations	***Coordination and evaluation of computer based works***	-
Wireless router configurations.	***Coordination and evaluation of computer based works***	-
Network attacks. DNS attacks	***Coordination and evaluation of computer based works***	-
Installing and configuring a firewall and NIDS	***Coordination and evaluation of computer based works***	-
Installing and configuring Antivirus and antimalware applications	***Coordination and evaluation of computer based works***	-
Web applications security. Cookies	***Coordination and evaluation of computer based works***	
Cross-site scripting, cross-site request forgery	***Coordination and evaluation of computer based works***	
SQL injection	***Coordination and evaluation of computer based works***	
Auditing the security of a computer system network	***Coordination and evaluation of computer based works***	
Project	***Coordination and evaluation of computer based works***	

References

1. Ed Skoudis, Tom Liston. Counter Hack Reloaded. ed. 2, Prentice Hall, 2006
2. Michael Howard, David LeBlanc, John Viega. 24 Deadly Sins of Software Security. McGraw-Hill, 2009

9. **Corroboration of course contents with the expectations of the epistemic community's significant representatives, professional associations and employers in the field of the academic programme**

A good knowledge if security issues is mandatory for every computer system/network administrator in order to design and deploy a safe working IT environment.
Also computer programmers especially those who work in the field of WEB applications must know the security related issues regarding WEB programming.

10. **Assessment**

Activity	10.1 Evaluation criteria	10.2 Evaluation methods	10.3 Percentage of final grade
10.4 Course	*Final evaluation:*	***Final evaluation:*** *Project presentation.*	50%
10.5 Seminar/laboratory	*Continuous assessment*	***Continuous assessment:***	50%
10.6 Minimum performance standard: 5			

Note: ***Please see also the alignment 5 (Requisites), related to compulsory attendance of the practical classes. Also, a student who doesn't attend the Final examination, can not get a final mark even if he/she has a mark for continuous assessment. The assessment scale is from 1 to 10, and 5 is minimum to pass the exam.***

Submission date Course leader signature Seminar tutor signature

Date of approval by Department members Department director signature