COURSE OUTLINE

(1) GENERAL

SCHOOL	ENGINEERING		
ACADEMIC UNIT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDIES	UNDERGRADUATE		
COURSE CODE		**SEMESTER**	**6th**
COURSE TITLE	Information Technology Security		

INDEPENDENT TEACHING ACTIVITIES if credits are awarded for separate components of the course, e.g. lectures, laboratory exercises, etc. If the credits are awarded for the whole of the course, give the weekly teaching hours and the total credits	**WEEKLY TEACHING HOURS**	**CREDITS**
Lectures	3	
Laboratory exercises	1	
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).	4	5

COURSE TYPE general background, special background, specialised general knowledge, skills development	GENERAL BACKGROUND, SCIENTIFIC AREA
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	GREEK (Instruction and Examination)
IS THE COURSE OFFERED TO ERASMUS STUDENTS	YES (in ENGLISH)
COURSE WEBSITE (URL)	

(2)

(2) LEARNING OUTCOMES

Learning outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area
- Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B
- Guidelines for writing Learning Outcomes

The Information Technology Security course covers various topics of the scientific areas of Information Security, Computer Security, and Network and Communication Systems Security. The purpose of the course is to create a broad framework of theoretical and practical knowledge, and skills valuable for the student in the job market in fields related to the Security in Information Technology.

Upon successful completion of the course, the student:

- **will know the security problems in Information and Communications systems,**
- **will recognize vulnerabilities in information and communication systems,**
- **will be able to apply basic principles of security policy design,**
- **will know the security mechanisms that implement these policies,**
- **will be familiar with cases that implement security mechanisms in different Operating Systems,**
- **will have knowledge of Database Security,**
- **will know the different types of firewalls and how they are used and applied,**
- **will know authentication mechanisms, their role and importance,**
- **will be familiar with Computer Forensics and have knowledge of the tools that support them,**
- **will know cryptography and cryptanalysis, and finally,**
- **will have understood Intrusion Detection Systems, how they operate and detection techniques used.**

General Competences

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology	Project planning and management Respect for difference and multiculturalism Respect for the natural environment
Adapting to new situations	Showing social, professional and ethical responsibility and sensitivity to gender issues
Decision-making	Criticism and self-criticism
Working independently	Production of free, creative and inductive thinking
Team work	……
Working in an international environment	Others…
Working in an interdisciplinary environment	…….
Production of new research ideas	

- Examine, retrieve, analyze and synthesize data and information by utilizing necessary technologies
- Work independently
- Team work
- Project planning and management
- Work in an interdisciplinary environment
- Promoting free, creative and inductive thinking

(3)

(3) SYLLABUS

The course includes the topics described in the following list:

- IT Security Overview
- Cryptography I
- Cryptography II
- Operating Systems Protection
- Data Base Security
- Access Control
- Network and Distributed Systems Security
- Internet Security
- Intrusion Detection I
- Intrusion Detection II
- Computer Forensics
- Risk Analysis
- Security Management
- Legal and Ethical Issues

(4)

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY Face-to-face, Distance learning, etc.	Face to face
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY Use of ICT in teaching, laboratory education, communication with students	• Specialized software tools for vulnerability assessment, for cryptographic algorithms, for Computer Forensics, for Database Security, for Intrusion Detection, for Access Control. • Use of ICT in Course Teaching • Use of the Open eClass course management system, for distributing lecture notes and exercises for practice, and for communication with students.
TEACHING METHODS The manner and methods of teaching are described in detail. Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc. The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS	**ActivitySemester workload** Lectures 39 Laboratory Practice 13 Essays / Project 20 Independent Study 53 **Course total 125**

STUDENT PERFORMANCE EVALUATION Description of the evaluation procedure Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other Specifically-defined evaluation criteria are given, and if and where they are accessible to students.	I. Final theory written exam (70%), which includes: * Questions that combine knowledge and criticism, with complete justification and description of arguments, through which it is established the level of understanding of the topics. II. Laboratory exercises and written final lab exam: a total of 30% score that derives from individual laboratory projects, over the grade of the final theory written exam, when this is at least 5. For successfully qualifying the course, a minimum grade of 5.0 marks (of 10 in total) is mandatory in both written exams and projects evaluation.

(5)

(5) ATTACHED BIBLIOGRAPHY

- Suggested bibliography:

1. Σωκράτης Κάτσικας, Στέφανος Γκρίτζαλης, και Κωνσταντίνος Λαμπρινουδάκης (Επιστημονική Επιμέλεια), "Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο", Εκδόσεις Νέων Τεχνολογιών, 2021 (in greek).
2.
3. Stallings και Brown, Computer Security Principles and Practice, Third Edition 2015, Pearson, ISBN-10: 0-13-377392-2 ISBN-13: 978-0-13-377392-7.

4. Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Δικτύων Υπολογιστών, Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ ΟΕ, 2003, ISBN: 978-960-7530-45-5 (in greek).

5. Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8th edition 2020, ISBN-13: 978-0135764268.

6. Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., Ασφάλεια της Πληροφορίας, ΕΚΔΟΣΕΙΣ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΜΟΝ. ΕΠΕ, 2004, ISBN: 960-8105-66-8 (in greek).

7. Κάτσικας Σ.Κ., Γκρίτζαλης Δ., Γκρίτζαλης Σ., Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004 (in greek).

8. Κάττος Β., Στεφανίδης Γ., Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης, ΖΥΓΟΣ, 2003 (in greek).

9. Bishop M., Computer Security – Art and Science, Addison-Wesley, 2003.

10. Bishop M., Introduction to Computer Security, Addison-Wesley, 2005.

11. Buchmann J., Introduction to Cyptography, 2nd Ed., Springer, 2004.

12. Casey E., Handbook of Computer Crime Investigation – Forensic Tools and Technology, Academic Press, 2002.

13. Mitnick K.D., Simon W.L., The Art of Deception, John Wiley & Sons, 2002.

14. Oppliger R., Security Technologies for the World Wide Web, Artech House Inc., 2000.

15. Pfleeger C.P., LawrencePfleeger S., Security in Computing, Prentice Hall, 2003.

16. Pieprzyk J., Hardjono T., Seberry J., Fundamentals of Computer Security, Springer, 2003.

17. Proctor P.E., The Practical Intrusion Detection Handbook, Prentice Hall, 2001.

18. Riggs G., Network Perimeter Security – Building Defense In-Depth, Auerbach, 2004.

19. Schultz E.E., Shumway R., Incident Response – A Strategic Guide to Handling System and Network Security Breaches, New Riders Publishing, 2002.

20. Spitzner L., Honeypots – Tracking Hackers, Addison Wisley, 2003.

21. 19. Young S., Aitel D., The Hacker's Handbook – The Strategy behind Breaking into and Defending Networks, Auerbach, 2004.

(6)