COURSE OUTLINE

(1) GENERAL

SCHOOL	Science and Technology		
ACADEMIC UNIT	Science and Technology		
PROGRAMME OF STUDIES	MSc in Cybersecurity		
LEVEL OF STUDIES	Postgraduate		
COURSE CODE	CC01	SEMESTER	1
COURSE TITLE	Information Systems Security		
COURSE TYPE *Elective, compulsory*	Compulsory		
INSTRUCTOR(S)	Theory: Assoc. Prof. Konstantinos Rantos		

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
	3,75	6
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		
TEACHING ACTIVITIES BREAKDOWN	WEEKLY HOURS	
Theory	3,75	
Add rows if necessary. The organisation of teaching and the teaching methods used are described in detail at (d).		

COURSE TYPE *general background, special background, specialised general knowledge, skills development*	Special background
PREREQUISITE COURSES:	-
LANGUAGE OF INSTRUCTION and EXAMINATIONS:	English
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes
COURSE WEBSITE (URL)	https://elearn-ucips.ihu.gr/

(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*

On completing the course, the student will be able to:

● Understand the role of cybersecurity frameworks.

- Propose protection mechanisms according to international frameworks and best practices.
- Explain the risk management process.
- Understand how to apply a risk assessment method.
- Understand how to use main cryptographic mechanisms.
- Describe cyber threat management best practices
- Describe the components of a zero-trust architecture.

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*
Adapting to new situations	*Respect for difference and multiculturalism*
Decision-making	*Respect for the natural environment*
Working independently	*Showing social, professional and ethical responsibility and sensitivity to gender issues*
Team work	*Criticism and self-criticism*
Working in an international environment	*Production of free, creative and inductive thinking*
Working in an interdisciplinary environment	*......*
Production of new research ideas	*Others...*
	....

- Search for, analysis and synthesis of data and information, with the use of the necessary technology
- Decision Making
- Teamwork
- Production of free, creative, and inductive thinking

(3) SYLLABUS

This course provides an introduction to the foundational aspects of cybersecurity and computer security. Most modern organisations face security and privacy risks that threaten their valuable assets. It is imperative to design secure and privacy-aware information systems that protect against these threats. This course provides a wide range of skills and knowledge of existing technologies, security and privacy principles to develop the professional skills and experience needed for information systems security. The topics covered include:

- Cybersecurity Essentials.
- Information Security Management Systems.
- Cybersecurity Frameworks.
- Information Security Risk Management.
- Applied Cryptography.
- Threats and Vulnerabilities.
- Cyber Threat Information.
- Zero Trust Architectures.

(4) TEACHING and LEARNING METHODS - EVALUATION

DELIVERY *Face-to-face, Distance learning, etc.*	Hybrid: Face to face, asynchronous online and synchronous distance learning
USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY *Use of ICT in teaching, laboratory education, communication with students*	**Use of ICT in Teaching** During the educational process, various risk management and applied cryptography tools are used, along with training material from the industry and other material available at the e-learning platform. The hybrid teaching method involves synchronous learning with the support of the videoconferencing tool Zoom.

	Students are taught a variety of tools related to the course content and material, mainly related to information security risk management and applied cryptography. **Use of ICT in Communication with students** • The course material (slides, scientific articles, exercises, etc.) is posted on the course page at the e-learn platform (Moodle). • Use of Moodle Forums announcements. • Live video meetings via Zoom. • Contact via email.
TEACHING METHODS *The manner and methods of teaching are described in detail.* *Lectures, recitation, 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*	(see table below)

Activity	Semester workload
Lectures	30 hrs.
Asynchronous online training	30 hrs.
Project	20 hrs.
Exams	2 hrs.
Non-Directed Study	78 hrs.
Course total	**150 hrs.**

COURSE MATERIAL ARRANGEMENT	**Theory/Recitation**

Information Security Management Systems	2 hrs.
Cybersecurity Frameworks	2 hrs.
Information Security Risk Management	8 hrs.
Threats and Vulnerabilities	3 hrs.
Cyber Threat Information	3 hrs.
Applied Cryptography	8 hrs.
Zero Trust Architectures	4 hrs.

| **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 | Language of Evaluation: English

Evaluation Procedure:
● Successful attendance of asynchronous online training material (20%)
● Individual project (20%):
   ○ Information security risk management (10%)
   ○ Applied cryptography (10%)
● Written Exams (60%). Methods of evaluation:
   ○ Open-ended questions
   ○ Multiple choice questions

Students need to achieve a passable grade on assignments and the written exam in order to successfully complete their course obligations.
The evaluation procedure is announced to the students during the first lecture and is also accessible at the e-learn platform throughout the entire semester. |
| **STUDENT OBLIGATIONS**
Compulsory attendance of lectures, labs, recitations, compulsory participation in midterms, exams, compulsory delivery of homework, projects, etc. | ● Compulsory attendance of lectures
● Compulsory attendance of asynchronous online training material
● Compulsory delivery of project |

	● Compulsory participation in the exams

(5) ATTACHED BIBLIOGRAPHY

- Suggested Textbooks
1. Security standards applying to all European Commission information systems https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en
2. ENISA Threat and Risk Management https://www.enisa.europa.eu/topics/threat-risk-management
3. NIST Computer Security Resource Center https://www.nist.gov/cyberframework https://csrc.nist.gov/Projects/riskmanagement
4. Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 –Project 645421, D5.4, ECRYPT-CSA, 02/2018. https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf
5. Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 5, NIST, 05/2020. https://doi.org/10.6028/NIST.SP.800-57pt1r5
6. Cryptographic Mechanisms: Recommendations and Key Lengths, TR-02102-1 v2020-01, BSI, 03/2020. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-021021.pdf?__blob=publicationFile
7. Block Cipher Modes, NIST. https://csrc.nist.gov/projects/block-cipher-techniques/bcm
8. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, ISBN: 0-8493-8523-7, October 1996, 816 pages.
9. Cybersecurity and Infrastructure Security Agency (CISA) -Cybersecurity Division, Zero Trust Maturity Model, June 2021, Version 1.0, https://www.cisa.gov/zero-trust-maturity-model
10. Scott W. Rose, Oliver Borchert, Stuart Mitchell, Sean Connelly, NIST SP 800-207, Zero Trust Architecture, August 2020, https://doi.org/10.6028/NIST.SP.800-207
11. Implementing a Zero Trust Architecture (2nd Preliminary Draft), https://csrc.nist.gov/publications/detail/sp/1800-35/draft