COMMUNICATIONS AND INFORMATION SECURITY REGULATORY FRAMEWORK

(1) GENERAL

SCHOOL	ENGINEERING		
ACADEMIC UNIT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDIES	UNDERGRADUATE		
COURSE CODE	ICE-7306	**SEMESTER**	9TH
COURSE TITLE	COMMUNICATIONS AND INFORMATION SECURITY REGULATORY FRAMEWORK		

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**	**ECTS**
Lectures	3	
Tutorials	1	
Labs		
Add rows if necessary. The organization of teaching and the teaching methods used are described in detail at 4	**4**	**5**

COURSE TYPE background, special background, specialized general knowledge, skills development	Specialised General Knowledge, Skills Development
PREREQUISITES	-
LANGUAGE OF INSTRUCTION	Greek (Instruction, Examination)
IS THE COURSE OFFERED TO ERASMUS STUDENTS	Yes (In English)
COURSE WEBSITE (URL)	

(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 course aims to deepen the students' knowledge in topics which relate to emerging regulatory issues on Cybersecurity. The objectives of the course include national and international regulatory frameworks, Risk Analysis and Management methodologies in the industry, Ethical and Political issues on Cybercrime and Cyberespionage, etc.

Upon successful completion of this course each student will be able to:

- Gain specialised knowledge on advanced concepts regarding Privacy-Confidentiality- Trust-Data Protection, as well as the regulatory/legislative framework that enforces their protection
- Understand, comprehend, deepen and combine knowledge in advanced topics on Ethics in regard to the study and development of communications and information systems architectures
- Combine knowledge and to manage complicated issues on the legislative and the ethical dimension of attacks in communications and information systems
- Utilise knowledge on advanced security topics and methodologies for conducting Risk Analyses and Management, developing Security Policies and Business Continuity Plans

- Resolve advanced industry problems by comprehending and utilising knowledge on Cybersecurity roadmaps
- Combine knowledge on national and international strategies on Cybersecurity and to develop opinions on these strategies' technical, political and social perspective
- Deepen in advanced technical and regulatory topics on Cybercrime and Cyberespionage in the global political scene
- Have proven knowledge and comprehend the emerging challenges on the field of Cybersecurity in national and international level to construct the required background for developing and applying novel ideas on the subject
- Compare, evaluate, and develop opinions, and clearly notify their conclusions on different regulatory/legislative/institutional approaches in regard to communications and information security
- Benefit elevated knowledge on methodological approaches which may offers to continue their study path in an autonomous manner

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
Adapting to new situations
Decision-making
Working independently
Team work
Working in an international environment
Working in an interdisciplinary environment
Production of new research ideas

Project planning and management
Respect for difference and multiculturalism
Respect for the natural environment
Showing social, professional and ethical responsibility and sensitivity to gender issues
Criticism and self-criticism
Production of free, creative and inductive thinking
……
Others…
…….

- Work independently / Teamwork
- Retrieve, analyse and synthesise data and information by utilising necessary technologies
- Adapt to new situations
- Decision-Making
- Project planning and management
- Work in an international environment
- Work in an interdisciplinary environment
- Advance of new research ideas
- Advance of free, creative and inductive thinking

(3) SYLLABUS

- Basic Concepts of Regulatory Frameworks
- National and International strategies on Cybersecurity
- Ethical and legislative dimension on attacks in communications and information systems
- Cybercrime and violation in the Cyberspace
- Cyberespionage and Information Security
- Regulatory Framework and Adjustments regarding Security and Privacy within the EU (Instruments, Bodies, Acts, Institutional Freedoms)
- Authorities on Security and Privacy
- Regulatory and Legislative Bodies on Security and Privacy
- Review of the International and European regulatory and institutional framework on Privacy-Confidentiality-Trust-Data Protection
- Regulatory and Social dimensions of Information
- Data protection by default/by design

- Cybersecurity Directives (E.U. GDPR, U.S. HIPPA, APAC, P.R.C. CSL, etc.)
- Human Security (Social Engineering, Social Networks, Social Norms, FERPA and CAL Directives, etc.)
- Privacy on the Internet
- Business Security (Sarbanes-Oxley, GLBA, NIST SP 800-37 Rev.2, National Cybersecurity and Critical Infrastructure Protection Act of 2014, etc.)
- Risk Analysis and Management Methodologies
- International Standards on Security Assessment, Security Policy, Business Continuity Plan (ISO/SEC 27001-27005, 14971, etc.)
- Bilateral, transnational, and international agreements on Cybersecurity Policies
- Cybersecurity roadmaps in the industry

(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	• Use of ICT in Course Teaching • Use of the Open eClass learning-management system, for distributing lecture notes, exercises for practice and for communicating with the 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	

Activity	Semester workload
Lectures	39
Tutorials	13
Project	30
Independent Study	43
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	**I.** Written exams (accounts 70% of the total course mark) which consist of: - Short answer questions - Multiple choice questions - Real-life problems resolution **II.** Essays // Projects (accounts 30% of the total course mark) For successfully qualifying the course, a minimum grade of 5.0 marks (of 10 in total) is mandatory in the written exams.

patient, art interpretation, other Specifically-defined evaluation criteria are given, and if and where they are accessible to students.	

(5) ATTACHED BIBLIOGRAPHY

Suggested bibliography:

GREEK

1. Labrinoudakis K, Mitrou L., Gkritzalis S. and Katsikas S., “Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα” [Privacy protection and Information & Communications Technology: Technical and Law Topics], 2010
2. Donos P. Mitrou L., Mittleton F., Papakonstantiou Ev., “Η Αρχή Προστασίας Προσωπικών Δεδομένων και η επαύξηση των δικαιωμάτων”, [Data Protection Authority, and Rights Augmentation], 2003
3. Katsikas S., “Διαχείριση Ασφάλειας Πληροφοριών” [Information Security Management], 2014
4. Gkritzalis D., “Αυτονομία και Πολιτική Ανυπακοή στον Κυβερνοχώρο” [Autonomy, and Political Disobedience in the Cyberspace], 2019

ENGLISH

1. Guiora, A., “Cybersecurity: Geopolitics, law, and policy” (paperback), NY: CRC Press, 2017
2. Tropina, T. and Callanan, C., “Self- and Co-regulation in Cybercrime, Cybersecurity and National Security”, Cham: Springer International Publishing, 2015
3. Grady, M. and Parisi, F., “The Law and Economics of Cybersecurity”, Cambridge: Cambridge University Press, 2006

- Supplementary bibliographic resources:

1. Savvakis Ch. et al., “Νέες Τεχνολογίες και Συνταγματικά δικαιώματα” [Emerging Technologies and Constitutional Rights], 2004

- Scientific Journals:

1. Cybersecurity, Springer
2. Journal of Cyber Policy, Taylor & Francis
3. Journal of National Security Law and Policy (JNSLP)
4. European Cybersecurity Journal (ECJ)

- Internet resources:

1. http://www.dpa.gr/ - Hellenic Data Protection Authority (HDPA)
2. https://ec.europa.eu/info/law/law-topic/data-protection_en - Data Protection Topics (European Commission)
3. https://www.enisa.europa.eu/ - European Union Agency for Cybersecurity
4. http://www.nist.gov – National Institute of Standards and Technology (US)
5. http://www.itu.int – International Telecommunication Union