UNIVERSITY OF PIRAEUS
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
DEPARTMENT OF DIGITAL SYSTEMS

Distance Learning Master of Science
Advanced Cybersecurity Technologies and Governance by Research

Study Guide
of the M.Sc.
«Advanced Cybersecurity Technologies and Governance by Research»
Academic year 2026-2027

Piraeus, March 2026

TABLE OF CONTENTS

1 The University of Piraeus....6

1.1 History....6

1.2 Organisational Structure....7

1.2.1 Rectorate....7

1.2.2 Organizational Chart....7

2 The Department of Digital Systems....10

2.1 Department Objectives....10

2.2 Students' professional privileges....10

2.3 Personnel....10

2.4 Administrative Staff....12

2.5 Infrastructure....13

3 The M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»....14

3.1 Subject - Purpose....14

3.2 Master's Degree....16

3.3 Structure and Bodies of the M.Sc.....16

3.4 Categories and Number of Admitted Students....19

3.5 Criteria and Selection Process for Admission to the M.Sc.....20

3.6 Evaluation of Candidates....22

3.7 Application Fees, Tuition Fees and Payment Method....23

3.8 Enrolment of Postgraduate Students....24

3.9 Duration of Studies-Conditions of Attendance....24

3.10 European Credit Transfer and Accumulation System (ECTS)....25

3.10.1 Credits of the Study Programme....25

3.10.2 Workload....25

3.10.3 Award of ECTS Credits....26

3.10.4 Transfer of ECTS Credits....26

3.11 Language of the Programme....26

3.12 Teaching Staff....26

3.12.1 Director of the M.Sc.....27

3.12.2 Teaching Staff....28

3.13 Professional Career Prospects of Graduates....34

3.14 Academic Calendar....36

3.15 Courses Outline....36

3.15.1 Courses offered per semester....37

3.15.1.1 1st Academic Semester....37

3.15.1.2 2nd Academic Semester 38
3.15.1.3 3rd Academic Semester 38
3.15.2 Courses descriptions per academic semester 38
3.15.2.1 1st Academic Semester 38
3.15.2.1.1 Research Methodology 38
3.15.2.1.2 Privacy and Data Protection 40
3.15.2.1.3 Cybersecurity Governance 41
3.15.2.1.4 Network Security 42
3.15.2.1.5 IoT Security 44
3.15.2.2 2nd Academic Semester 46
3.15.2.2.1 Study of the Research Area 46
3.15.2.2.2 Digital Wellbeing in Cyber-space 47
3.15.2.2.3 Offensive Security 51
3.15.2.2.4 Forensics 52
3.15.2.2.5 Secure Autonomous Systems 53
3.15.2.2.6 Cybersecurity: Attack, Defence, and Operational Practice 55
3.15.2.2.7 Cybersecurity in Industrial Scenarios 56
3.15.2.2.8 Cybersecurity in the Political Domain: Internal and External Dimensions) 57
3.15.2.3 3rd Academic Semester 62
3.15.2.3.1 Master Thesis 62
3.16 Learning Outcomes 63
3.16.1 Knowledge 63
3.16.2 Skills 64
3.16.3 Competences 64
3.17 Preparation of assignments 65
3.18 Preparation of the Master Thesis through Erasmus 65
3.19 Digital Services 65
3.19.1 Digital Services of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research» 65
3.19.1.1 M.Sc., Department of Digital Systems, and University of Piraeus websites 65
3.19.1.2 Course Management System «LEFKIPPOS» (Open eClass) 66
3.19.1.3 Virtual Campus 66
3.19.1.4 Master's Program Electronic Application Submission System «ARISTYLLOS» 67
3.19.1.5 Student information & academic evaluation portal for the M.Sc. «SIS-PORTAL» 67
3.19.1.6 Synchronous Teaching (Microsoft Teams) 68
3.19.1.7 University Laboratories 69
3.19.1.8 M.Sc. Graduates: Electronic Registration in the Club Alumni 69
3.19.2 Electronic Services of the Academic Unit 69
3.19.2.1 University of Piraeus Website 69
3.19.2.2 Master's Students Dining 69

3.19.2.3 University of Piraeus Library 70
3.19.2.4 Healthcare 71
3.19.2.5 European Health Insurance Card (EHIC) 71
3.19.2.6 University Medical Center 71
3.19.2.7 Counseling Center 71
3.19.2.8 Volunteer Team - Kerykes 72
3.19.2.9 Cultural Groups at the University of Piraeus 72
3.19.2.10 Sports Activities at the University of Piraeus 72
3.19.2.11 Digital Notice Board 72
3.19.2.12 Teaching and Learning Support Center (TLSC) 72
3.19.3 Guidelines for activating the electronic services of the M.Sc. *73*
3.19.3.1 Creation and management of the institutional account 73
3.19.3.2 "mypassword" Service 74
3.19.4 Electronic Services of the Ministry of Education, Religious Affairs and Sports *74*
3.19.4.1 Academic Identity Card Online Service 75
3.19.4.2 DELOS 365 Service 76
3.19.5 Supportive services for master's students of the University of Piraeus *76*
3.19.5.1 Software Distribution Website 76
3.19.5.2 Wireless Network Services and Virtual Private Networks (VPN) 77
3.19.6 Supportive services for master's students from external providers *77*
3.20 Rights and Obligations of Postgraduate Students 77
3.21 Awarding of scholarships 79
3.22 Student Mobility 79
3.23 Academic Advisor 79
3.24 Management of Students' Complaints and Appeals 80
3.25 Evaluation of postgraduate students 80
3.25.1 Description of the assessment of learning outcomes system *80*
3.25.2 Learning Outcomes *81*
3.25.3 Evaluation System *81*
3.25.4 Adaptation of the evaluation system for master's students with serious conditions and learning difficulties 84
3.26 Procedures and criteria for the selection of teaching staff 84
3.27 Graduation Ceremony/ Oath-Taking 85
3.28 Infrastructure and Funding of the M.Sc. Program 86
3.29 Evaluation of the M.Sc. Program 86
3.30 Access to the Premises of the University of Piraeus 88
3.30.1 Access to the University Premises by Public Transportation *88*
3.30.2 Accessibility Infrastructure for Persons with Disabilities *89*

3.31 Contact Information 90
3.31.1 Department's Academic Secretariat *90*
3.31.2 M.Sc. Program's Secretariat *90*
3.31.3 M.Sc. Program's Social Media *91*
4 APPENDICES 92
4.1 Appendix 1: Application for Admission to the Master Program 92
4.2 Appendix 2: Recommendation Letter Template 98
4.3 Appendix 3: Mobility of students and staff Regulation (ERASMUS+ & ERASMUS+ International) 101
4.4 Appendix 4: Regulation on the Functioning of the Academic Advisor 101
4.5 Appendix 5: Regulation for the Management of Students' Complaints and Appeals 101
4.6 Appendix 6: Regulations for the Preparation of Assignments 101
4.7 Appendix 7: Master Thesis Preparation Regulation 101

1 The University of Piraeus

1.1 History

The University of Piraeus was founded as a "School of Industrial Studies" in 1938 by the Association of Industrialists and Craftsmen, in accordance with the Law N.5197/1931 and the A.N. 28/1936, in association with the Federation of Public Limited Companies Greece intending to provide economic, legal and technical education to industrial executives. Then:

- In 1945 it was renamed to "Higher School of Industrial Studies" and its purpose was that of the systematic theoretical and practical training of administrative personnel.
- In 1949, the organization was complete (law 1245/49).
- In 1958, it was renamed to Graduate School of Industrial studies of Piraeus. From then on, courses lasted four years and degrees awarded were equivalent to those of other universities.
- Since 1966, the school has been operating as a public entity.
- From the academic year 1971-1972, studying at the School provided two paths to select from the second year: Economic Science and Business Administration.
- The Department of Statistics and Insurance Science was founded during the academic year 1977-1978.
- With law 1268/82 the school initially operated with one Department. In 1984 (law 43/1984) the school was organized to include three departments: Economic Science, Business Administration and Statistics and Insurance Science.
- In June 1989, Law 377/89 prescribed the renaming of the School to "University of Piraeus", and the creation of three more academic departments, namely:
    - Banking and Financial Management.
    - Maritime Studies
    - Technology and Production Systems
- In the academic year 1990-1991, two of the three departments started to operate:
    - the Department of Banking and Financial Management and
    - the Department of Maritime Studies
- The Department of Technology and Production Systems was launched in the academic year 1991-1992 and was later (2002) renamed to "Department of Industrial Management and Technology" according to law 113/30-4-2002/ Government Gazette: 95.
- The Department of Informatics began operating in the academic year 1992-1993.
- The Department of Technological Education was launched in academic year 1999-2000 and was renamed in 2002 to "Department of Computer Education and Digital Systems" and in 2009 to "Department of Digital Systems".

- The Department of International and European Studies was launched in the academic year 2000-2001.
- The Department of Tourism Studies was launched in the academic year 2017-2018.

1.2 Organisational Structure

1.2.1 Rectorate

Rector of the University of Piraeus is Professor Sfakianakis Michail, Professor of the Department of Business Administration.

Vice Rectors:

- Vice-Rector for Research and Lifelong Education: Kyriazis Demosthenes, Professor of the Department of Digital Systems of the School of Information and Communication Technologies
- Vice-Rector for Finance, Planning and Development: Sofianopoulou Styliani, Professor of the Department of Industrial Management and Technology of the School of Maritime and Industrial studies
- Vice-Rector for Academic and Administrative Affairs: Roukanas Spyridon, Professor of the Department of International and European Studies of the School of Economics, Business and International Studies
- Vice-Rector for International Relations and External Relations: Veropoulou Georgia, Professor at the Department of Statistics and Insurance Science of the School of Finance and Statistics

1.2.2 Organizational Chart

University of Piraeus:

- Rector
    - Vice-Rector for Research and Lifelong Education
        - Center for Continuing Education and Lifelong Learning (Unit)
        - Directorate of Support for University Bodies
            - Department of University Authorities
            - Department of Planning and Documentation
        - Special Account for Research Funds - Financial and Administrative Support Unit
            - Department of Program Management and Monitoring
            - Department of Administrative and Technical Support
            - Department of Financial Management
        - Department of IT (Department of Computerisation)

        - Network Management Center (Network Operations Center)
    - Vice-Rector for Finance, Planning and Development
        - General Directorate of Administration Services (see below)
        - Library Department
        - Department of Technical Projects (Department of Infrastructure)
    - Vice-Rector for Academic and Administrative Affairs
        - General Directorate of Administration Services (see below)
        - Center for Teaching and Learning Support
        - Quality Assurance Unit (MODIP)
    - Vice-Rector for International Relations and External Relations
        - International Relations Office
    - Security and Protection Unit (Department)
    - Legal Department
    - Strategic Planning Unit (Department)
- Senate
    - Secretariat of the Board of Directors and Senate
- Board of Directors
    - Executive Director
    - Secretariat of the Board of Directors and Senate
- Judicial Office of the Legal Council of the State
- Internal Audit Unit
- Other Services
    - Printing Office
    - Publications and Editions Office
    - Clinic and Counselling Center
- Directorate of Information Communication Technology and Technical Works
    - Department of IT (Department of Computerization)
    - Department of Technical Projects (Department of Infrastructure)
    - Network Management Center (Network Operations Center)
- Directorate of Support for University Bodies
    - Department of University Authorities
    - Department of Planning and Documentation

General Directorate of Administration Services:

- Directorate of Administration
    - Department of Teaching Staff
    - Department of Administrative Personnel and Administration
    - Department of Protocol – Processing and Archives
- Secretariats of Departments and Schools

    - School of Economics, Business and International Studies
        - Secretariat of the Department of Economics
        - Secretariat of the Department of Business Administration
        - Secretariat of the Department of International and European Studies
        - Secretariat of the Department of Tourism Studies
    - School of Maritime and Industrial Studies
        - Secretariat of the Department of Maritime Studies
        - Secretariat of the Department of Industrial Management and Technology
    - School of Finance and Statistics
        - Secretariat of the Department of Banking and Financial Management
        - Secretariat of the Department of Statistics and Insurance Science
    - School of Information and Communication Technologies
        - Secretariat of the Department of Informatics
        - Secretariat of the Department of Digital Systems
- Directorate of Studies and Student Welfare
    - Department of Undergraduate Studies
    - Department of Postgraduate Studies
    - Department of Student Care
        - Accessibility Center for individuals with disabilities
    - Student Support Unit (Department)
- Financial Directorate
    - Accounting Department
    - Department of Payroll
    - Procurement and Property Department

2 The Department of Digital Systems

2.1 Department Objectives

The Department of Digital Systems of the University of Piraeus was founded in 1999 and covers two important fields:

- Network-Oriented Systems and Services
- Telecommunication Systems and Networks

The transition to the Society of Information requires the emergence of skilled scientists capable of contributing to the development, implementation and management of modern digital technology systems.

On this basis, the Undergraduate Programme of Studies of the Department provides the following majors of study:

- Major in "Telecommunications & Networks" (T&N)
- Major in "Software & Data Systems" (SDS)
- Major in "Computational Infrastructures & Services" (CIS)
- Horizontal Major in "Security" (SEC)
- Horizontal Major in "Teaching Qualification" (ICT)

The Department of Digital Systems offers a four-year Undergraduate Programme of Studies which corresponds to 240 credits of the European Credit Transfer and Accumulation System (ECTS) and awards, upon successful completion, a Bachelor degree in "Digital Systems".

2.2 Students' professional privileges

The Undergraduate Studies Programme is designed to prepare scientists capable of successfully coping with complex design, development and implementation problems of modern digital technology. Graduates of the Department have already staffed IT and telecommunications companies in the public and private sectors, both in Greece and abroad, as well as educational organizations. Also, many of our graduates follow a research path both in Greece and abroad.

2.3 Personnel

I. Professors

- Angeliki Alexiou
- Panagiotis Demestichas
- Christos Doulkeridis
- George Efthymoglou
- Michael Filippakis
- Stefanos Gritzalis
- Maria Halkidi

- Athanasios Kanatas
- Dimosthenis Kyriazis
- Konstantinos Lambrinoudakis
- Ilias Maglogiannis
- Apostolos Meliones
- Foteini Paraskeva
- Andriana Prentza
- Symeon Retalis
- Angelos Rouskas
- Demetrios Sampson
- Nikitas-Marinos Sgouros
- George Vouros
- Christos Xenakis

II. Associate Professor

- Demosthenes Vouyioukas

III. Assistant Professors

- Andreas Menychtas
- Orestis Telelis

IV. Emeritus Professors

- Sokratis Katsikas
- Ioannis Maniatis
- George Vassilacopoulos

V. Laboratory Teaching Staff

- Aristi Galani
- Dimitrios Gkotzos
- Evangelos Haleplidis
- Vassiliki Koufi
- Eleni-Laskarina Makri
- Christos Manousopoulos
- Konstantinos Moutselos
- Angeliki Panou
- Eleftheria Stougiannou

VI. Specialized Technical and Laboratory Staff

- Katerina Poupouza

2.4 Administrative Staff

Academic Secretariat

Secretariat Group E-mail : gramds@unipi.gr

- Paraskevi Antoniou (Chief)
  - Tel.: +30-210-4142235
  - E-mail: panton@unipi.gr
- Sofia Skountzou
  - Tel.: +30-210-4142373
  - E-mail:sskountz@unipi.gr
- Ioannis Frentzas
  - Tel.: +30-210-4142426
  - E-mail: fretzas@unipi.gr
- Panagiotis Theodoropoulos
  - Tel.: +30-210-4142369
  - E-mail: ptheodor@unipi.gr

2.5 Infrastructure

The University of Piraeus is housed in its main building at 80 Karaoli & Dimitriou Street, where the administrative services, offices of part of the teaching and research staff, and teaching classrooms are located. In addition, it uses facilities in the building on Deligiorgi Street (Department of Industrial Management and Technology), in the building at 78 Tzamadou Street and Deligiorgi Street (teaching classrooms), in the building at 40 Karaoli & Dimitriou Street (Department of Maritime Studies and teaching classrooms), in the building at 78 Tzamadou Street (Student Restaurant), in the building at 91 A. Papanastasiou Avenue (University of Piraeus Research Center), in the building at 80 Zeas Street (Secretariat of the Department of Digital Systems), and in the building at 150 Androutsou Street (offices of the Teaching and Research Staff and laboratories of the Department of Digital Systems).

The Department of Digital Systems is housed in a privately owned building of the University of Piraeus located at 150 Androutsou Street, where six (6) fully equipped computer laboratories operate with a total capacity of one hundred and sixty (160) workstations for undergraduate and postgraduate students of the Department. The Department's laboratories operate on all working days from 09:00 to 21:00 and are equipped with modern laboratory equipment (hardware and software), which is continuously enriched and upgraded.

3 The M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»

The M.Sc. programme «**Advanced Cybersecurity Technologies and Governance by Research»** is established within the framework of the European project **EU-iNSPIRE** (EU **iN**novative multi-di**S**ci**P**linary **I**ndustry-focused cybersecurity education for upskilling and **R**eskilling the EU workforce**)** which started in January 2025, has a duration of four (4) years, and is funded under the programme DIGITAL-2023-SKILLS-05 (Grant Agreement No. 101190054). Specifically, for the first two (2) cohorts of operation, the organisational and operational costs of the M.Sc. programme, including the tuition fees for students from EU countries, are covered by the funding of this project.

The objectives of the EU-iNSPIRE project, and thus of the M.Sc. programme *"Advanced Cybersecurity Technologies and Governance by Research"*, are to address the multifaceted educational and professional specialisation needs that are critical for supporting the future Cyber Resilience ecosystem of the EU through an innovative triple approach:

- **Scientific development of ICT professionals**, enabling them to leverage cybersecurity technologies to enhance the resilience of processes, systems, and digital infrastructures.
- **Training of scientists in cyber risk protection**, including the application of mechanisms for the assessment of threats, vulnerabilities, and risks in cyberspace.
- **Empowerment of experts with specialized digital transformation knowledge**, enabling them to implement efficient and innovative solutions in cybersecurity compliance assessment processes.

The following Universities, that also serve as partners in the aforementioned project, are participating in this Master Program and have agreed to be actively involved in the educational process through their teaching staff:

- University of Piraeus (Greece),
- Technical University of Munich (Germany),
- University of Oslo (Norway),
- University of Malaga (Spain),
- Open University of Cyprus (Cyprus)

In addition, the École des Ponts Business School (France) will support the programme by providing distinguished professors to deliver targeted, seminar-style lectures.

3.1 Subject - Purpose

The widespread use of Information and Communication Technologies (ICT) is radically transforming the international social, economic, technological, political, and cultural environment, enabling the rapid creation, transfer, processing, and storage of large volumes of data. The intensification of the digitalization of activities carried out by citizens, businesses, and public administration significantly increases the attack surface

and the complexity of cybersecurity threats. Cyberattacks can affect economic stability, social cohesion, the operation of critical infrastructures, and, in certain cases, human life itself. At the same time, the modern regulatory framework of the European Union (indicatively: NIS2 2022/2555, DORA 2022/2554, GDPR 2016/679, e-Privacy 2002/58, Cybersecurity Act 2019/881) creates a dynamic environment of regulatory requirements that requires scientific analysis, evaluation, and well-documented support for policy and technological choices. This evolution creates new research challenges and scientific questions related both to the exploitation of data and to ensuring their integrity, confidentiality, and availability.

Within this context, the Postgraduate Programme (M.Sc.), which is interdisciplinary and cross-disciplinary in nature, focuses on the production of original scientific research in the fields of cybersecurity, data protection, and the governance of digital and information environments.

The purpose of the M.Sc. programme is to advance scientific knowledge through systematic and original research in the fields of cybersecurity technologies, data protection, and the governance of related environments. The programme aims to cultivate high-level researchers capable of designing, implementing, and publishing research with international impact, thereby contributing substantially to scientific progress and to the development of evidence-based policies and technological solutions.

Graduates of the M.Sc. will be able to pursue careers in academic and research institutions, research centers, international organizations, as well as in research and development (R&D) departments of public and private organizations, contributing to the production of new knowledge and innovation.

The objectives of the M.Sc. "Advanced Cybersecurity Technologies and Governance through Research", that is—according to epistemology—the means of achieving the aforementioned purpose, include:

- The systematic development of research capability in interdisciplinary fields related to cybersecurity, data protection, and the governance of digital ecosystems.
- In-depth study of advanced theoretical approaches, methodological tools, and analytical techniques—both quantitative and qualitative—that support the conduct of original research.
- The preparation of an independent research thesis of high scientific standard, capable of leading to publications in international scientific journals and/or peer-reviewed conference proceedings.
- The cultivation of the ability to critically analyze, evaluate, and synthesize international scientific literature.

- The development of innovative theoretical models, technological solutions, and/or regulatory approaches addressing the contemporary challenges of digital transformation.
- The strengthening of scientific ethics, research integrity, and compliance with international research standards.

All of the above make the M.Sc. programme extremely valuable, highly interesting, and remarkably competitive compared with leading research-oriented postgraduate programmes of similar thematic focus in other countries of the European Union. At the same time, it clearly differentiates itself from existing related postgraduate programmes in Greece, as described in detail in the following section, since it will be the only MSc programme in the country that addresses research topics in cybersecurity, data protection, and the governance of related environments exclusively in the English language. This is particularly significant given that the establishment of a research-oriented MSc programme in English, attracting postgraduate students from Greece as well as from other countries both within and outside the EU, is fully aligned with the institutional strategy of the University of Piraeus for internationalization and the development of innovative educational initiatives delivered in English.

3.2 Master's Degree

The M.Sc. awards a Master of Science Diploma in "*Advanced Cybersecurity Technologies and Governance by Research"*.

The Master's Degree Certificate (diploma) is an official public document, the format of which is determined by decision of the Senate. It is drawn up and awarded in both Greek and English. Master's Degree Programmes lead to a qualification at Level 7 of the European Qualifications Framework (EQF) and the National Qualifications Framework (NQF). The diploma is signed by the Rector, the Head of the Department, and the Department Secretary. The grade of the diploma is classified as follows: **5.00–6.49 GOOD**, **6.50–8.49 VERY GOOD**, and **8.50–10.00 EXCELLENT**.

The register of M.Sc. graduates is signed by the Department Secretary, the Head of the Department, and the Rector of the University. A Diploma Supplement, issued in both Greek and English, is attached to the diploma in accordance with the provisions of Article 15 of Law 3374/2005 (Government Gazette A' 189) and Ministerial Decision Ref. No. Φ5/89656/Β3/13.8.07 (Government Gazette Β' 1466).

3.3 Structure and Bodies of the M.Sc.

The competent bodies for the establishment, organization, and operation of the M.Sc., according to Law 4957/2022, are:

a) the Senate of the University
b) the Assembly of the Department
c) the Coordinating Committee (C.C.) of the M.Sc.
d) the Director of the M.Sc.

The responsibilities of the bodies of the M.Sc. are as follows:

1. The Senate is the competent body for matters of academic, administrative, and organizational nature concerning the M.Sc. programs. The Senate has the following responsibilities regarding the M.Sc. programs, as well as any others provided by the Internal Operating Regulation of the institution, provided these have not been specifically assigned by law to other bodies of the institution:
   - approves the establishment or modification of the founding decision of the M.Sc. program, as well as the content of these programs
   - approves or modifies the internal operating regulations of the M.Sc. programs
   - approves the extension of the duration of the M.Sc. programs
   - approves the establishment of collaborations with domestic or foreign institutions or research centers – institutes and technological bodies as defined in Article 13A of Law 4310/2014 (Government Gazette 258, Vol. A') for the organization of inter-institutional second-cycle study programs, as well as protocols for academic or research collaboration with domestic or foreign entities
   - decides on the termination of M.Sc. programs offered by the University
2. The Assembly of the Department is responsible for the organization, administration, and management of the M.Sc. and specifically:
   - submits a proposal to the Senate for the approval or modification of the founding decision of the M.Sc. program, as well as for the extension of the duration of the M.Sc. program
   - appoints the members of the Coordinating Committee (C.C.) of the Department's M.Sc. program
   - assigns teaching responsibilities to the instructors of the M.Sc. program
   - establishes committees for the evaluation of applications from prospective master's students and approves their enrollment in the M.Sc. program
   - establishes examination committees for the assessment of master's theses of the master's students and appoints the supervisor or co-supervisors for each postgraduate thesis
   - verifies the successful completion of studies in order to award the Master of Science Diploma
   - approves the program's financial and academic report, following the recommendation of the Coordinating Committee
   - exercises any other responsibility provided by the provisions of the Operating Regulation

By decision of the Department's Assembly, the responsibilities listed under items 4 and 5 may be delegated to the Coordinating Committee of the M.Sc. program (paragraph 2, Article 82 of Law 4957/2022).
Additionally, specific responsibilities of the Department's Assembly may be delegated to the Coordinating Committee for the more effective operation of the M.Sc. program, following the issuance of a relevant delegation decision.

3. The Coordinating Committee (C.C.) consists of the Director of the M.Sc. program and four (4) members of the Department's Faculty who have academic expertise relevant to the knowledge areas of the M.Sc. program and undertake teaching responsibilities within it. The members of the C.C. are appointed by the Department's Assembly for a two-year term, concurrent with the term of the Director. Emeritus Professors of the Department may also participate in the C.C., provided they teach in the M.Sc. program. The members of the C.C. are not entitled to any salary or compensation for the execution of the responsibilities assigned to them in relation to their duties. The C.C. is responsible for monitoring and coordinating the operation of the M.Sc. program and in particular:
   - prepares the initial annual budget of the M.Sc. program and its revisions, if the program has resources (Article 84 of Law 4957/2022), and submits it for approval to the Research Committee of the Special Account for Research Grants (SARG) of the University
   - prepares the program's financial and academic report and submits it for approval to the Department's Assembly
   - approves the execution of expenditures of the M.Sc. program
   - approves the granting of scholarships, remunerative or non-remunerative, in accordance with what is defined in the founding decision of the M.Sc. program and the Regulation for Postgraduate and Doctoral Studies
   - submits a proposal to the Department's Assembly regarding the allocation of teaching duties, as well as the assignment of teaching duties to categories of instructors (Article 83 of Law 4957/2022)
   - submits a proposal to the Department's Assembly for the invitation of Visiting Professors to cover teaching needs of the M.Sc. program
   - drafts a plan for modifications of the curriculum, and submits it to the Department's Assembly
   - submits a proposal to the Department's Assembly regarding the redistribution of courses across academic semesters, as well as issues related to the qualitative improvement of the curriculum
   - exercises any other responsibility provided by the provisions of the Operating Regulation.
4. The Director of the M.Sc. is selected from the faculty members of the Department, preferably holding the rank of Professor or Associate Professor and is appointed by

the Department's Assembly for a two-year term, which can be renewed without limitation. The Director of the M.Sc. is not entitled to any remuneration or compensation for performing the duties assigned to her/him in relation to the execution of her/his responsibilities. The Director of the M.Sc. has the following responsibilities:

1. Chairs the Coordinating Committee (C.C.), prepares the agenda, and convenes its meetings
2. Submits proposals concerning the organization and operation of the M.Sc. to the Department's Assembly.
3. Makes recommendations to the C.C. and other bodies of the M.Sc. and the University regarding the effective operation of the M.Sc.
4. Serves as the Scientific Coordinator of the program (in accordance with Article 234 of Law 4957/2022) and exercises the corresponding responsibilities.
5. Monitors the implementation of decisions made by the governing bodies of the M.Sc. and the Internal Regulations for Postgraduate and Doctoral Study Programs, as well as the spending of the M.Sc. budget.
6. Carries out any other responsibilities specified in the founding decision of the M.Sc.

By decision of the Research Committee, a Deputy Scientific Supervisor of the project/program may be appointed, if deemed necessary, following a decision of the Department's Assembly.

The administrative and secretarial support of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research» is undertaken by the Secretariat of the Department. Administrative staff who support the Master programmes outside their regular working hours at the University, as well as those assigned tasks related to the M.Sc., may be compensated for the services they provide.

3.4 Categories and Number of Admitted Students

Holders of a Bachelor degree from Higher Education Institutions (HEIs) in Greece or equivalent recognized institutions abroad are eligible for admission to the M.Sc., in accordance with the provisions of Law 4957/2022, as currently in force. All applicants must have sufficient knowledge of the English language, which is the language of instruction.

Members of Special Teaching Staff, Laboratory Teaching Staff, Specialized Technical and Laboratory Staff, and administrative personnel of the University may also apply. If, after the evaluation process, are accepted, they may be considered as exceeding the standard

admission capacity, and only one such individual per year may be admitted, in accordance with the Internal Regulations of the institution.

More specifically, the M.Sc. is addressed to graduates of Higher Education Institutions in Greece or equivalent institutions abroad. Indicatively, eligible applicants include graduates from: Departments of Informatics and Communications, Departments of Physical and Technological Sciences, Engineering Schools, Law Schools, Departments of Political Science and Public Administration, Departments of Management and Economics. Additionally, graduates of the National School of Public Administration and those from Military Academies of the Armed Forces and Security Forces are also eligible.

The M.Sc. admits eighty (80) students per academic year.

3.5 Criteria and Selection Process for Admission to the M.Sc.

The selection of admitted students to the M.Sc. is carried out in accordance with the provisions and regulations outlined in the Postgraduate Studies Regulation.

A call for applications for admission to the M.Sc. is issued and published on the Department's and the Institution's website, following a decision of the Department's Assembly. This announcement includes all relevant submission details. Applications and supporting documents must be submitted electronically or delivered to the Department Secretariat within the deadline stated in the call. This deadline may be extended by decision of the Department's Assembly.

Each applicant must submit the following:

1. Application form (a template is provided).(Appendix 1: Application for Admission to the Master Program).
2. Curriculum Vitae (CV).
3. Copy of degree/diploma or a certificate of completion of studies.
4. Academic transcript (that includes degree/diploma grade if the candidate has completed the studies).
5. Two letters of recommendation (a template is provided). (Appendix 2: Recommendation Letter Template).
6. Copy of Bachelor's or Diploma thesis (if applicable).
7. Scientific publications in peer-reviewed journals or conferences, or other publications (if applicable).
8. Proof of professional or research activity (if applicable).
9. Certificate of good knowledge of the English language.
10. Photocopy of passport or national identification document.
11. One photograph.

The Department's Assembly may specify additional required documents. The exact procedure is detailed in the call for applications.

For candidates holding a Bachelor from institutions abroad, verification will be conducted to ensure the institution is listed in the National Register of Recognized Foreign Institutions, as well as in the National Register of Recognized Foreign Degree Titles. In any case, foreign qualifications must be submitted and accepted in accordance with the applicable legal provisions.

Exceptionally, applications may be accepted from candidates who, by the application deadline, have not yet obtained their Bachelor degree. If selected, such candidates must submit either a certificate of study completion or an officially certified copy of their degree before enrollment in the M.Sc., otherwise, they will not be allowed to enroll. The same requirement applies to the certificate of English language competency.

The evaluation of candidates for the M.Sc. is conducted by a Candidate Evaluation Committee, which is composed of Faculty members of the M.Sc. and is established by decision of the Department's Assembly. The approval of Master's student registrations is also determined by the Department's Assembly.

The selection criteria, along with the details regarding how they are applied, are communicated to the applicants through the official call for applications for the M.Sc.

The criteria include, but are not limited to, the following:

- Academic degrees
- Grade point average of academic degrees
- Course grades —especially the grade of the undergraduate or diploma thesis— provided they are relevant to the subject matter of the M.Sc.
- Possession of a second degree/diploma or a postgraduate qualification
- Field and duration of professional or research experience
- Letters of recommendation from Faculty members of HEIs and/or employers
- Interview (remotely using digital tools)
- Additional criteria as defined by decision of the Department's Assembly

The Department's Assembly may establish an Additional Internal Examinations Committee, on the proposal of the Selection Committee, for all or some candidates. The Selection Committee determines the syllabus and timing of these examinations.

The selection procedure is conducted by the Selection Committee, which:

- compiles a complete list of all applicants,

- rejects candidates who do not meet the minimum criteria -where such criteria have been set by the Department's Assembly and are included in the M.Sc.'s Operating Regulation or whose dossier lacks any required document,
- invites to interview those candidates decided to be called; interviews are conducted by the Committee members remotely,
- organises any internal examinations deemed necessary for particular candidates,
- ranks the candidates by score and submits its recommendation for approval to the Department's Assembly

Successful candidates must enroll with the Department Secretariat within a deadline set by the Department's Assembly. In the event of a tie, **all** candidates who share the same score as the last successful candidate are deemed successful.

If one or more selected candidates do not enroll, an equal number of alternates will be invited -where available- to enroll in the Programme, according to their order in the approved ranking list.

3.6 Evaluation of Candidates

The evaluation of candidates for admission to the M.Sc. is conducted by the Candidate Evaluation Committee, composed of faculty members of the program and established by decision of the Department's Assembly. The Committee may include faculty members holding the rank of Professor. The evaluation process shall be carried out in accordance with the criteria and procedures stipulated in the Program's Regulations and shall include a remote personal interview conducted via approved digital communication platforms (e.g., MS Teams or equivalent). The approval of Master's student enrolments is also determined by the Department's Assembly.

The first evaluation phase is preliminary and is based on the information derived from the submitted supporting documents.

The criteria used in this phase are the following:

Criteria	Importance
Background knowledge	30%
Overall skillset	30%
Critical thinking capability	20%

The total points from the first evaluation phase carry a weighting of 80% in the final score.

The second phase consists of a personal interview of all candidates, in which each one's particular aptitude, potential, and overall academic profile are assessed. This phase carries a weighting of 20%.

3.7 Application Fees, Tuition Fees and Payment Method

For all cohorts of operation of the M.Sc. Programme, within the application process the applicants pay an application fee of two hundred (200) euros. This fee is non-refundable for all candidates, regardless of the evaluation outcome.

For the first two (2) cohorts of operation of the M.Sc. Programme, the tuition fees of postgraduate students coming from Greece and the other EU countries are fully covered by the European project EU-iNSPIRE (EU iNnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce), financed under the DIGITAL-2023-SKILLS-05 programme (Grant Agreement No. 101190054). For postgraduate students coming from non-EU countries, the tuition fees for these cohorts are five thousand euros (5.000€).

From the third (3rd) cohort of operation of the M.Sc. Programme onward, the tuition fees of postgraduate students coming from Greece and the other EU countries are five thousand euros (5.000€), while for postgraduate students coming from non-EU countries the tuition fees are seven thousand euros (7.000€).

According to the Postgraduate Studies Regulation, tuition fees are paid in two equal instalments: the first instalment upon the announcement of those admitted to the M.Sc. Programme, to reserve the place (September), and the second instalment at the beginning of the second academic semester. Payment of application and tuition fees to the Special Account for Research Funds of the University of Piraeus may also be made by credit or debit card.

From the third (3rd) cohort of operation onwards the rules governing the exemption of students from tuition fees shall follow the applicable legislation. Under current legislation, a number of students not exceeding thirty percent (30%) of the total cohort, who are not nationals of third countries (Note: A "third country" is any country outside the European Economic Area (EEA). The EEA includes the 28 EU Member States, as well as Iceland, Norway, and Liechtenstein), are entitled to a full exemption from tuition fees, provided that specific criteria are met. These criteria are defined in the Ministerial Decision *"Regulation of issues regarding the exemption of students of Postgraduate Programmes of Greek Higher Education Institutions from tuition fees"* (No. 108990/Z1/08.09.2022, Government Gazette B' 4899), which specifies the required documentation, and the Ministerial Decision *"Determination of the amount corresponding to the national median*

equivalent disposable income (individual and seventy percent (70%) of family income)" (No. 84560/Z1/27.07.2023, Government Gazette 4837/01.08.2023). Additionally, for full exemption from tuition fees, according to Article 86 of Law 4957/2022, students must also meet the academic excellence criterion from their first cycle of studies, namely holding at minimum a bachelor degree with a grade equal to or higher than 7.5/10. For students granted tuition fee exemption, any fees already paid will be refunded in full. This exemption applies exclusively to enrolment in one (1) postgraduate programme organized by a Greek Higher Education Institution.

3.8 Enrolment of Postgraduate Students

The enrolment of admitted postgraduate students shall take place within the deadlines announced by the M.Sc. Director.

Prior to enrolment, the candidate shall:

- be informed that, under the new European General Data Protection Regulation (EU) 2016/679, which entered into force on 25 May 2018, a unified legal framework for the protection of personal data has been established across all EU Member States. In this context, the candidate is informed that, in accordance with applicable legislation governing the enrolment of successful applicants to postgraduate programmes, the University of Piraeus maintains personal data of its postgraduate students. Furthermore, the candidate is informed that the University of Piraeus collects additional information from its postgraduate students, which may include personal data. All the collected data are maintained and processed for the purposes of enrolment, subsequent academic administration, communication with the student's designated contacts in cases of emergency, and for ensuring access to electronic services throughout the duration of studies.
- provide consent for the maintenance and processing of their personal data for all the above-mentioned purposes.
- declare that all information and supporting documents submitted are accurate, truthful, and genuine copies of the originals.
- confirm that she/he has read the "*Postgraduate Studies Regulation*" and provide written confirmation that she/he accepts the rules governing the operation of the programme.
- provide the email address at which she/he wishes to receive personalized correspondence.

Enrolment information is published on the M.Sc. programme's website.

3.9 Duration of Studies-Conditions of Attendance

The duration of the M.Sc. Programme leading to the award of the Master's Degree is three (3) academic semesters.

The first two (2) semesters comprise taught courses, while the third semester is devoted to the preparation of the Master's Thesis. Throughout the cycle of studies, students will also be notified of any seminar-type lectures that are scheduled.

The maximum permitted time for completion of studies is five (5) academic semesters. Students are entitled to one (1) additional semester beyond the standard duration in order to complete their studies. Moreover, the Department's Assembly, on the C.C.'s recommendation, may grant an extension beyond these (3+1) semesters, following a student's application, only for serious reasons beyond the student's control (e.g. professional obligations, health issues). The application must be accompanied by the relevant supporting documents.

Postgraduate students may submit a reasoned request for a temporary suspension of studies not exceeding two (2) consecutive semesters. Suspension semesters do not count towards the maximum study period. A suspension is granted upon the student's application, the C.C.'s recommendation and a decision of the Department's Assembly. The application must state the reasons, the requested suspension period and include any supporting evidence.

3.10 European Credit Transfer and Accumulation System (ECTS)

The European Credit Transfer and Accumulation System (ECTS) is a tool of the European Higher Education Area (EHEA) aimed at increasing the transparency of studies and, consequently, improving the quality of higher education. Its purpose is to strengthen and facilitate the processes of academic recognition among cooperating institutions in Europe that operate under different national education systems, through the use of simple and applicable mechanisms.

3.10.1 Credits of the Study Programme

The number of credits assigned to each course of the M.Sc. programme reflects the workload required of a postgraduate student to achieve the objectives of an educational component, in accordance with the intended learning outcomes and the knowledge, skills, and competences to be acquired upon its successful completion. Workload includes all scheduled learning activities, such as lectures, seminars, study, preparation of assignments, examinations, and similar activities.

3.10.2 Workload

Workload refers to the estimated amount of time a postgraduate student is typically expected to devote in order to complete all learning activities, such as attending lectures,

seminars, preparing assignments, undertaking independent study, and taking examinations, required to achieve the intended learning outcomes.

Sixty (60) ECTS credits correspond to the workload of one academic year of full-time study within a formal learning framework and the associated learning outcomes. For the courses of the specific M.Sc. programme, one (1) ECTS credit is equivalent to twenty-five (25) hours of student workload.

3.10.3 Award of ECTS Credits

To be awarded the M.Sc. degree, students must accumulate 90 ECTS credits. The number of credits assigned to each course component is based on its weight in terms of the workload that the students have to undertake in order to achieve the intended learning outcomes.

3.10.4 Transfer of ECTS Credits

The ECTS credits awarded in one programme may be transferred to another programme offered by the same or by a different institution. Such a transfer shall take place only if the degree-awarding institution recognizes the credits and the associated learning outcomes. The M.Sc. programme *"Advanced Cybersecurity Technologies and Governance by Research"* complies with the European Credit Transfer and Accumulation System (ECTS) and has a formal procedure for the transfer and recognition of academic course credits. This procedure is applied in all cases where educational activities listed in the Study Guide of the M.Sc. programme are of equivalent content and comparable level to educational activities in which the postgraduate student has been successfully examined during previous studies, whether those studies were completed or not.

3.11 Language of the Programme

The teaching language for all courses is English. The bibliography includes scientific articles and textbooks in English.

3.12 Teaching Staff

The teaching staff of the M.Sc. programme *"Advanced Cybersecurity Technologies and Governance by Research"* includes distinguished professors from universities in Greece and abroad, doctoral-level researchers, as well as prominent executives from Independent Authorities, public organisations, and private sector enterprises. All members of the teaching staff possess exceptional academic qualifications, originate from the fields of Information and Communication Technologies and Cybersecurity, and bring substantial expertise and unique professional experience gained in internationally advanced scientific environments.

As part of the M.Sc. programme, the following universities have agreed to participate in the educational process: the Technical University of Munich (Germany), the University of Oslo (Norway), the University of Malaga (Spain), and the Open University of Cyprus (Cyprus). In addition, the Business School of École des Ponts (France) will support the programme by providing distinguished professors for targeted, seminar-style lectures. With the active support of these universities, eminent professors and researchers will contribute to the teaching of the programme, thereby enhancing its international and interdisciplinary character.

3.12.1 Director of the M.Sc.

Prof. Costas Lambrinoudakis holds a B.Sc. (Electrical and Electronic Engineering) from the University of Salford (1985), an M.Sc. (Control Systems) from the University of London (Imperial College -1986), and a Ph.D. (Computer Science) from the University of London (Queen Mary and Westfield College - 1991). From 1998 until 2009 he has held teaching position with the University of the Aegean, Department of Information and Communication Systems Engineering, Greece. Currently he is a Professor at the Department of Digital Systems, University of Piraeus, Greece. From 2015 he is Director of the Systems Security Lab, while for the period 2015-2020 he served as Head of the Department. For the period 2012-2015 he was a member of the board of the Hellenic Authority for Communication Security and Privacy, while from 2016 he serves on the board of the Hellenic Data Protection Authority. His current research interests are in the areas of Information and Communication Systems Security and of Privacy Enhancing Technologies. For many years he is working on issues related to the protection of personal data and the compliance of information systems to the National and European Legislation. He is an author of more than 120 scientific publications in refereed international journals, books and conferences, most of them on ICT security and privacy protection issues. He has served as program committee chair of 15 international scientific conferences and as a member on the program and organizing committees in more than 200 others. Also he participates in the editorial board of two international scientific journals and he acts as a reviewer for more than 35 journals. He has been involved in many national and EU funded R&D projects in the area of Information and Communication Systems Security. (https://www.ds.unipi.gr/en/faculty/clam-en/)

3.12.2 Teaching Staff

Stefanos Gritzalis is a Professor of Information and Communication Systems Security, at the Lab. of Systems Security, Dept. of Digital Systems, University of Piraeus, Greece (2019+) and Director of the Postgraduate Programme "MSc in Law and Information & Communication Technologies" (2020+). He is a Member of the Board of the Hellenic Authority for Communication Security and Privacy (2020+). He is a Member of the Board of the National Commission for Human Rights (2024+) He was the Rector of the University of the Aegean, Greece (2014-2018). He has acted as Special Secretary for the Hellenic Ministry for Administrative Reform and Electronic Governance (2009-2012). Previously, he was a Professor at the University of the Aegean, Greece, School of Engineering, Dept. of Information and Communication Systems Engineering, and member of the Info-Sec-Lab Laboratory of Information and Communication Systems Security (2002-2019). He was the Head of the Dept. of Information and Communication Systems Engineering (2005-2009), Deputy Head of the Dept. of Information and Communication Systems Engineering (2012-2014), and Director of the Lab. of Information and Communication Systems Security (2005-2009). He holds a BSc in Physics, an MSc in Electronic Automation, and a PhD in Information and Communications Security from the Department of Informatics and Telecommunications, University of Athens, Greece. His published scientific work includes more than 14 books (including the book "Digital Privacy: Theory, Technologies and Practices", co-edited by A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. De Capitani di Vimercati, Auerbach Publications, Taylor and Francis Group) and 37 book chapters. Moreover, his work has been published in 336 papers (151 in refereed journals and 185 in the proceedings of international refereed conferences and workshops). He has co-authored papers with more than 200 researchers from 30 countries during the last 30 years. The focus of his publications is on Information and Communications Security and Privacy. His most frequently cited papers have more than 11.000 citations, h-index=55, i10-index=178, as measured by Google Scholar. He is listed, again, in the top 2% of the most cited researchers in the ICT domain around the globe, as ranked by researchers from Stanford University and published by Elsevier (September 2024). He acts as Area Editor for the prestigious "IEEE Communications Surveys and Tutorials" journal (IF=46.7 in the Clarivate JCR report, ranked No. 1 in 120 journals of Telecommunications area, and No. 1 in 259 journals of Computer Science, Information Systems area). He is the Editor-in-Chief or Editor or Editorial Board member in 35 journals and a Reviewer in more than 80 scientific journals. He has acted as Guest Editor in 35 journal special issues, he has been General Chair or Program Committee Chair in more than 50 international conferences and workshops, he has served as a Program Committee Member of more than

600 international conferences and workshops. He has been the advisor of 17 completed PhD theses; these scientists are now working in academia and industry (TU Delft, University of the Aegean, University of Crete, ENISA, European Commission JRC, Volvo group, Hellenic Ministry of Digital Governance, TEIRESIAS SA, Hellenic Statistical Authority, Hellenic Civil Aviation Authority, Hellenic Ministry of Education etc.). Moreover, he has acted as external evaluator/examiner for more than 60 PhD students from Germany, Italy, Spain, India, Pakistan, Greece, etc. Moreover, he has supervised more than 150 Master Theses and 300 First Diploma / BSc Theses. He has been involved in several National and EU funded R&D projects receiving research and development grants of over € 6.0 million. He has acted as External Evaluator for research proposals submitted to: ERC European Research Council, Swiss National Science Foundation SNSF, Italian Ministry of University and Research, The Netherlands Organisation for Scientific Research, Belgian Fund for Scientific Research, Czech Science Foundation, FFG Austrian Research Promotion Agency, ETH Zurich Research Commission, Croatian Ministry of Science and Education, Slovenian Research Agency, South Africa's National Research Foundation, Qatar Foundation – Qatar National Research Fund, Cyprus Research Promotion Foundation, The University of Nicosia Research Foundation in Cyprus, Hellenic Foundation for Research and Innovation, Hellenic General Secretariat for Research and Technology, Hellenic Ministry of Economy and Development ESF Operational Programme "HR Development, Education and Life Long Learning" etc. Moreover, he has acted as member of the 2015 IEEE Technical Recognition Award Selection Committee for the "IEEE Communications & Information Security Technical Recognition Award". His professional experience includes senior consulting and researcher positions in a number of private and public institutions. He was elected twice as Member of the Board (Secretary General, Treasurer) of the Greek Computer Society. He acts as member of the Hellenic Association for Information Systems AIS – Hellenic Chapter, the Association for Computing Machinery ACM, the Institute of Electrical and Electronics Engineers IEEE and the IEEE Communications Society "Communications and Information Security Technical Committee". (https://www.ds.unipi.gr/en/faculty/sgritz-en/).

Dr. **Christos Kalloniatis** holds a PhD from the Department of Cultural Technology and Communication of the University of the Aegean, a master degree on Computer Science from the University of Essex, UK and a Bachelor degree in Informatics from Technological Educational Institute of Athens. Currently he is a full time Professor and head of the Department of Cultural Technology and Communication of the University of the Aegean and director of the Privacy Engineering and

Social Informatics (PrivaSI) research laboratory. He is a member of board of the Hellenic Data Protection Authority and former member of the board of the Hellenic Authority for Communication Security and Privacy. His main research interests are the elicitation, analysis and modelling of security and privacy requirements in traditional and cloud-based systems, the analysis and modelling of forensic-enabled systems and services, Privacy Enhancing Technologies and the design of Information System Security and Privacy in Cultural Informatics. He is an author of several refereed papers in international scientific journals and conferences and has served as a visiting professor in many European Institutions. Prior to his academic career he has served at various places on the Greek public sector including the North Aegean Region and Ministry of Interior, Decentraliastion and e-Governance. He is a lead-member of the Cultural Informatics research group as well as the privacy requirements research group in the Department of Cultural Technology and Communication of the University of the Aegean and has a close collaboration with the Laboratory of Information & Communication Systems Security of the University of the Aegean. He has served as a member of various development and research projects. (https://kalloniatis.aegean.gr/).

Professor **Charalambos Vrasidas** is a Professor of Learning Technologies and Innovation and Associate Dean for e-learning at the University of Nicosia. He is the co-founder and Executive Director of CARDET (Center for the Advancement of Research and Development in Educational Technology), a Non-Governmental non-profit research and development center based in Cyprus with partners around the world. He graduated from the Pedagogical Academy of Cyprus (PAC) in June 1989. PAC was the official teachers' college that prepared teachers for elementary schools, and which has now become the University of Cyprus. In September 1991, he was appointed as an elementary school teacher. After working for a year in that position, he was awarded a Fulbright scholarship to pursue a Bachelors degree in the U.S. While in the US he received a B.S. in Photo/Multimedia with a minor in Film, from Western Illinois University (WIU). He then continued for a Masters in Education with emphasis on Instructional Technology and Telecommunication, also at WIU. In August 1996 he joined the Ph.D. program in Educational Media and Computers at Arizona State University and received his PhD in May 1999. (https://www.unic.ac.cy/vrasidas-charalambos/).

Dr. **Marinos Papaioakeim** is a researcher specialising in international relations, diplomacy, and defence and security, with a particular focus on the role of small states in security governance and defence diplomacy. He holds a PhD in Diplomacy and International Relations from the University of Cyprus, where his doctoral thesis examined the use of

defence diplomacy by small states in protracted conflicts. His research interests include, among others, security, military and defence diplomacy, hybrid threats, policy, and soft power. Dr Papaioakeim obtained his MA in Diplomacy and Foreign Policy from Lancaster University (UK), following a BA in History from the University of Cyprus. He has worked as a Research Associate at the School of Law at the University of Nicosia and served as Director of the Royal Commonwealth Society Cyprus. He has also held teaching and research roles as a Teaching Assistant and Special Scientist at the Department of Social and Political Sciences at the University of Cyprus. In addition, he has served as a lecturer and tutor at various academic institutions, delivering courses on diplomacy, international relations, conflict, security, and defence. He is currently employed at CARDET as a Senior Researcher, Project Manager, and Head of Department, where he manages several projects, particularly in the field of security. He also serves as a Research Fellow at the Diplomatic Academy of the University of Nicosia and the Institute of Politics and Democracy. (https://ucy.academia.edu/MarinosPapaioakeim).

Dr.-Ing. **Mohammad Hamad** leads the "Security for IoT and Autonomous Systems" research group in the Embedded Systems and Internet of Things group in the Faculty of Electrical Engineering and Information Technology at the Technical University of Munich (TUM). Before this, Dr.-Ing. Hamad received his Ph.D. in Computer Engineering (Dr.-Ing.) from TU Braunschweig in 2020. (https://www.ce.cit.tum.de/en/esi/staff/hamad/).

Audun Jøsang is Professor of cybersecurity at the University of Oslo, as well as adjunct professor at QUT in Australia. Prof. Jøsang is widely known for his research on trust and reputation systems in digital environments, such as online marketplaces and social media. One of Jøsang's key contributions is the development of Subjective Logic, a mathematical framework for reasoning under uncertainty, which has applications in areas like risk assessment, decision-making, artificial intelligence and the analysis of trust in social networks. This work is widely used in both academia and industry. Prof. Jøsang has an MSc in Information Security from Royal Holloway College, University of London, and an MSc in Telecommunications from NTNU where he also obtained his PhD. Books authored by Prof. Jøsang are Subjective Logic: A Formalism for Reasoning Under Uncertainty, and Cybersecurity: Technology and Governance. (https://www.mn.uio.no/ifi/english/people/aca/josang/).

Laszlo Erdodi lives in Oslo, Norway, where he is Associate Professor at the University Oslo (UiO) and also at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU). Laszlo Erdodi has 15+ years of experience in offensive security with numerous ethical hacking projects including specific tasks such as exploit development and power grid attacks. His main research fields are reinforcement learning aided cyber-attacks and power grid security. He is the head coach of the Norwegian student.
(https://www.mn.uio.no/ifi/english/people/aca/laszloe/index.html).

Dr. **Cristina Alcaraz** (F) is an Associate Professor at the Computer Science Department of the University of Malaga (UMA). She obtained her PhD in Computer Science by UMA in 2011, and her M.Sc. degree in Computer Science by the same university in 2006. She was awarded two highly competitive postdoctoral fellowships, Marie-Curie in 2012 under the COFUND program and Ramón-y-Cajal in 2015, and was a guest researcher at NIST (2011–2012, USA), visiting later the Royal Holloway (2012–2014 under the Marie-Curie Confund postdoctoral fellowship), UCBM (2017, Rome) and Neurosoft (2019 and 2022, Athens). Dr. Alcaraz, ranked among the top 2% of scientists since 2020-present, has published 95+ papers (with 40 publications indexed in JCR – 20-Q1, 15-Q2, 5-Q3) with interest in the security of cyber-physical systems, Industry 5.0/4.0, Industrial IoT, digital twins and aerospace networks, focusing her research on situational awareness, advanced detection, and resilience. She is IEEE OT Department Editor, Associate Editor of 7+ influential journals on security, such as the IEEE Transactions on Industrial Informatics, IEEE Tran. on Dependable and Secure, Int. Journal of Critical Infr. Protection, International Journal of Information Security, Distributed Ledger Technologies (ACM), IEEE Networking Letters, among others. In the academic context, she regularly teaches cybersecurity related to network security and industrial security, both at the undergraduate and master's levels. It should also be noted that Dr. Alcaraz received the 'Special Mention for Teaching Quality' and the 'Teaching Excellence' from the International University of Andalusia in 2023 and 2024, respectively. Dr. Alcaraz also received the recognition of "Women in Homeland Security" from the IEEE SMC TC on Homeland Security in 2021, and she is Vice-Chair of IEEE ComSoc SIG on Green Digital Twin Network. (https://www.nics.uma.es/cristina-alcaraz/).

Professor **Stavros Stavrou** holds a Ph.D. degree in Telecommunications from the University of Surrey (U.K.). His area of expertise spans areas in Communication Networks, Telecommunication Systems and Cybersecurity. He has published extensively in peer reviewed publications, has graduated several Ph.D. students in topics related to his above research areas, and has managed a large number of research projects as a Primary Investigator (PI) from research councils, government organizations and industrial collaborations. His current research interests span through different topics between layer 1 and 3 of the OSI model. He has contributed towards numerous technical reports and he is the patent holder of a mobile phone jammer. He has been the author/co- author and principal investigator of a number of successful research proposals, targeting research councils and industry. Professor Stavrou is the first elected chairman of the Cybersecurity Configuration of the European Security and Defence College, and a member of its Executive Academic Board. He is also a Fellow of the Higher Education Academy U.K.). (https://www.ouc.ac.cy/index.php/en/profiles/stavros-stavrou).

Dr. Eliana Stavrou holds a Ph.D. in Computer Science (Cybersecurity) from the University of Cyprus and a Master in Advanced Information Technologies from the same university. Dr. Stavrou is performing applied research in the area of cybersecurity education to address the challenges relevant to developing cybersecurity capabilities. Specifically, she is developing specialized educational and training curricula, and realistic practical activities, using innovative pedagogies and educational technologies to achieve effective teaching and learning. Dr. Stavrou has a special interest in the development of cyber resilience competencies, empowering people to anticipate, defend, recover from and adapt to cyber-attacks, through the promotion of a cyber situational awareness culture. In this context, her investigations focus on threat profiling aspects in different environments e.g., SMEs, critical Information Systems (IS), etc., to identify the attack exposure and to improve workforce and ISs capabilities. Primary sources of threat information and classification informing her investigations, include industrial cybersecurity frameworks such as MITRE ATT&CK matrixes, and threat intelligence information shared by the cyber community. Moreover, she is working towards bridging the skills shortage in cybersecurity by highlighting the multidisciplinary nature of cybersecurity and attracting people with different backgrounds to work in this area. Beyond upskilling the workforce, she also has a special interest to improve the cyber resilience capabilities of citizens. To this end, she is developing educational content and practical activities to improve citizens' cybersecurity situational awareness, and to promote a culture of best practices, starting from an early childhood, e.g., engaging kids through STEM. She is also investigating security challenges in the Internet of Things (IoT), developing security solutions across the IoT ecosystem. Dr.

Stavrou is a member of several working groups and advisory boards related to cybersecurity capabilities development, research and innovation. She has published a number of scientific papers at premier international journals and conferences and has been the principle investigator of a number of ICT and cybersecurity-related R&D projects funded by national, European and international funding programmes. (https://www.ouc.ac.cy/index.php/en/profiles/98-eliana-stavrou).

Adamantini Peratikou holds a PhD in Parallel Processing and Optimization Algorithms, a BSc in Computing from the University of Portsmouth, and a Postgraduate Certificate in Technology. She is a member of the Cybersecurity and Telecommunications Research Lab (CTRL) of the Open University of Cyprus, where she is currently working in various funded projects in the field of Cybersecurity and Networking. The past couple of years, part of her research work is related to Cyber Ranges and Cybersecurity training. She has published several papers in international peer reviewed conferences and journals in the areas of Cyber Ranges, Networks and Interconnection Architectures. She has served as a reviewer in a number of international conferences. She is in the technical programme committee for IEEE-ICC GCSN symposium, IEEE-CIT and IEEE Greencom for the past 7 consecutive years. Dr. Peratikou has experience in teaching at undergraduate and postgraduate level. (https://www.ouc.ac.cy/index.php/en/profiles/99-adamantini-peratikou).

3.13 Professional Career Prospects of Graduates

During the course of studies in the M.Sc. programme *"Advanced Cybersecurity Technologies and Governance by Research"*, students acquire knowledge and practical experience that enhance their career prospects and support their entry into a wide range of employment sectors. Specifically, they develop highly specialised knowledge and skills that address the increasing needs of both the public and private sectors in issues of cybersecurity, data protection, and governance of related environments.

In January 2023, the World Economic Forum announced the greatest global risks to humanity, categorised as Environmental, Geopolitical, Social, and Technological. According to that study, the most significant technological risk was considered to be the spread of cybercrime and the absence of cybersecurity. In a similar study in January 2024, the World Economic Forum reported that cyberattacks ranked as the fifth greatest global risk. Most recently, in January 2025, it identified digital attacks, digital surveillance, and online espionage as among the most significant technological risks worldwide.

According to data from the European Commission, Digital EU, and the Security Union, as analysed by PriceWaterhouseCoopers in 2020, the annual cost of cybercrime was

estimated at €5.5 trillion, double the cost in 2015. This amount exceeded estimated revenues from the global drug trade. If cybercriminals were considered a state, they would rank among the G20, with the 13th largest GDP in the world. Cybersecurity Ventures expects the cost of cybercrime to grow annually by 15%, reaching €10.5 trillion by the end of 2025—effectively making cybercrime the world's third-largest economy after the United States and China (https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/)

In Greece, a 2023 study by Allianz Global Corporate recorded cybersecurity incidents as the third greatest risk for the country, following the energy crisis and the inability to achieve sustainable macroeconomic growth. According to Eurostat, 22.2% of businesses in the EU (18% in Greece) have detected and addressed various security incidents. Additionally, according to the European Union Agency for Cybersecurity (ENISA), expenditure on cybersecurity by public and private sector entities amounts to approximately 7% of their overall ICT spending.

Regarding the labor market situation in Greece and internationally, both for ICT in general and cybersecurity in particular, the figures are striking. In the United States, President Joe Biden stated emphatically in August 2021 that "…half a million cybersecurity jobs are unfilled" (https://www.reuters.com/world/us/cyber-threats-top-agenda-white-house-meeting-with-big-tech-finance-executives-2021-08-25/). In the European Union, a study entitled Women in Cybersecurity reported that "The Cybersecurity field is suffering from a massive skills shortage. The gap, predicted to hit 1.8 million globally by 2022 and 350,000 in Europe alone. The gap is exacerbated by lack of female representation – with women comprising only 11% of the workforce, according to the 'Women in Cybersecurity' research. For Europe, the percentage is even lower – 7%. The involvement of women is an untapped resource. It is unlikely that we will close this gap without better gender balance" (https://www.iamcybersafe.org/s/). Other reputable studies identify specialized domains within cybersecurity that professionals in both public and private organizations need to prioritize.

In Greece, the percentage of professionals working in ICT is the lowest in Europe, representing only 2.5% of the workforce compared to the European average of 4.6%. According to research conducted in 2024 by Deloitte on behalf of the Federation of Hellenic Information Technology & Communications Enterprises (SEPE), the Greek labour market will require 300,000 ICT graduates by 2030 to contribute to the country's digital transformation. For the period 2023–2030, an additional cumulative demand of 120,000–140,000 ICT specialists is expected, which translates into a need for 15,000–16,000 additional specialists per year. Current annual supply from university graduates is 8,000–8,500, leaving an annual gap of 7,000–7,500 ICT graduates beyond the projected output of Greek universities.

All of this occurs in a national context marked by a sharp increase in electronic fraud in recent years. Recently, the President of the newly established National Cybersecurity Authority, the competent public entity for related matters, publicly acknowledged the difficulty of finding and attracting professionals with the appropriate knowledge and skills in cybersecurity and data protection.

Based on the above, it is evident that the labour market in Greece and the EU, in both the private and public sectors, continues to have a strong and growing demand for professionals with knowledge and skills in cybersecurity and data protection. Consequently, the employment prospects of graduates of the M.Sc. programme «**Advanced Cybersecurity Technologies and Governance by Research»,** primarily in Greece, but also across the EU—are exceptionally positive. Furthermore, through the application of modern teaching methods and case studies, graduates also acquire critical transversal ("soft") skills in effective communication, problem-solving, teamwork, time management, adaptability, and critical thinking.

3.14 Academic Calendar

The academic calendar is posted on the M.Sc. website at the beginning of each academic year and is updated whenever changes occur.

3.15 Courses Outline

The M.Sc. Programme begins in the winter academic semester of each academic year (September). To obtain the Master's Degree, students must accumulate a total of ninety (90) ECTS credits. During their studies, postgraduate students are required to attend and successfully complete postgraduate courses, engage in research activity and/or internship or other practical training, and prepare a Master's Thesis.

The organization of the educational process of the Postgraduate Program (M.Sc.) is carried out using methods of synchronous and asynchronous distance learning:

- **Synchronous distance learning** is an educational method implemented through technological mediation (videoconferencing environment), where the instructor and the learners interact from different locations but at the same time, with the possibility of two-way communication and real-time sharing of multimodal content (slides, videos, etc.). **The percentage of synchronous distance learning activities in the Postgraduate Program corresponds to 28.3% of the total ECTS credits of the courses.**
- **Asynchronous distance learning** is an educational method implemented through an integrated technological environment (platform) for asynchronous education, where the instructor and the learners interact from different locations and at different times. In particular, interaction takes place between a) instructor –

learner, b) learner – educational material, and c) learners. **The percentage of asynchronous distance learning activities in the Postgraduate Program corresponds to 20.4% of the total ECTS credits of the courses.**

Non-guided learning activities -individual and/or group study and exercises for each course- are supported through remote access to an appropriate asynchronous distance-learning platform (e.g. e-Class) and to the Library's digital services. **The percentage of non-guided educational activities in the Postgraduate Program (M.Sc.) corresponds to 51,3% of the total ECTS credits of the courses**.

Courses are organized by academic semester, taught on a weekly basis, and conducted entirely in the English language.

3.15.1 Courses offered per semester

The courses offered each semester are described below. In addition, postgraduate students will be informed well in advance about seminar-style lectures that may be scheduled.

3.15.1.1 1st Academic Semester

In the 1st semester students will need to attend one obligatory course and two of the four optional courses available.

Course Code	Course Title	Type	ECTS
DS-ACTG-A1	Research Methodology	Obligatory	15
DS-ACTG-001	Privacy and Data Protection	Optional	7,5
DS-ACTG-002	Cybersecurity Governance	Optional	7,5
DS-ACTG-003	Network Security	Optional	7,5
DS-ACTG-004	IoT Security	Optional	7,5
Total (one obligatory and two optional courses)			**30**

3.15.1.2 2nd Academic Semester

In the 2nd semester students will need to attend one obligatory course and two of the seven optional courses available.

Course Code	Course Title	Type	ECTS
DS-ACTG-B1	Study of the Research Area	Obligatory	15
DS-ACTG-005	Digital Wellbeing in Cyber-space	Optional	7,5
DS-ACTG-006	Offensive Security	Optional	7,5
DS-ACTG-007	Forensics	Optional	7,5
DS-ACTG-008	Secure Autonomous Systems	Optional	7,5
DS-ACTG-009	Cybersecurity: Attack, Defence, and Operational Practice	Optional	7,5
DS-ACTG-010	Cybersecurity in Industrial Scenarios	Optional	7,5
DS-ACTG-011	Cybersecurity in the Political Domain: Internal and External Dimensions	Optional	7,5
Total (one obligatory and two optional courses)			**30**

3.15.1.3 3rd Academic Semester

Course Code	Course Title	Type	ECTS
DS-ACTG-C1	M.Sc. Thesis	Obligatory	30

3.15.2 Courses descriptions per academic semester

3.15.2.1 1st Academic Semester

3.15.2.1.1 Research Methodology

COURSE SYLLABUS

- Introduction to Scientific Research and Cybersecurity
  - The role and importance of scientific research.
  - Research approaches in the natural and technological sciences.
  - Research as a driver of innovation in Cybersecurity.
  - The life cycle of a research project.
- Research Paradigms and Methodological Approaches

    - Quantitative, qualitative, and mixed methodologies.
    - Research strategies (experimental, descriptive, exploratory).
    - Case studies of research in Cybersecurity.
- Defining the Research Problem and Formulating Hypotheses
    - Identifying research gaps and challenges.
    - Formulating research questions, objectives, and hypotheses.
    - Developing a conceptual framework for research in Cybersecurity.
- Literature Review and Analysis
    - Techniques for searching scientific literature.
    - Use of databases (IEEE Xplore, Scopus, ACM DL).
    - Critical evaluation and synthesis of information.
- Management and Organization of References
    - Use of reference management tools (Zotero, Mendeley).
    - Creation and standardization of bibliographic references (IEEE, APA).
    - Development of an annotated bibliography.
- Research Study Design
    - Research design, variables, and sampling.
    - Types of studies: experimental, comparative, case studies.
    - Methodological design in Cybersecurity research.
- Data Collection and Research Tools
    - Data collection methods (logs, surveys, simulations).
    - Measurement and data storage tools.
    - Reliability and validity in data collection.
- Data Analysis and Statistical Processing
    - Basic statistical methods.
    - Use of tools (SPSS, R, Python).
    - Interpretation of results.
- Qualitative Methods and Content Analysis
    - Qualitative analysis techniques (thematic, content analysis).
    - Tools for qualitative analysis (NVivo).
    - Applications to socio-technical issues in Cybersecurity.
- Research Ethics and Academic Integrity
    - Ethical issues in Cybersecurity research.
    - GDPR, data management, anonymity, and informed consent.
    - Intellectual property rights and avoidance of plagiarism.
- Scientific Writing and Presentation of Research Results
    - Structure of a scientific paper.

    - Writing techniques and academic style.
    - Creation of figures, tables, and appendices.
- Presentation and Defense of Research Work
    - Preparation of a scientific presentation.
    - Oral defense techniques.
    - Use of visual aids (PowerPoint, LaTeX, Prezi).
- Development of a Research Proposal
    - Composition of a complete research proposal.
    - Presentation and evaluation by supervisors.
    - Preparation for the research thesis.

RECOMMENDED BIBLIOGRAPHY

- Creswell, J. W., & Creswell, J. D. (2023), Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (6th ed.), SAGE Publications.
- Oates, B. J. (2006), Researching Information Systems and Computing, SAGE Publications.
- Easterbrook, S. M., Singer, J., Storey, M. A., & Damian, D. (2008), Selecting Empirical Methods for Software Engineering Research, Guide to Advanced Empirical Software Engineering, Springer.
- Rainer, A., & Lock, R. (2020), Doing Your Research Project in the Information Sciences, Routledge.
- Yin, R. K. (2018), Case Study Research and Applications: Design and Methods (6th ed.), SAGE Publications.
- Kothari, C. R., & Garg, G. (2019), Research Methodology: Methods and Techniques (5th ed.), New Age International Publishers.
- Stallings, W., & Brown, L. (2021), Computer Security: Principles and Practice (5th ed.), Pearson.Requirements Engineering, Springer

3.15.2.1.2 Privacy and Data Protection

COURSE SYLLABUS

- Introduction to Privacy and GDPR Principles
- Legal and Regulatory Framework
- Privacy Governance Model
- GDPR Compliance Requirements
- Privacy Policies
- Risk Assessment and Management
- Data Protection Impact Assessment

- Privacy by Design and by Default
- AI and Personal Data
- Privacy Enhancing Technologies (PETs)
- Privacy Awareness
- Cyber Insurance and Personal Data
- Online Marketing and Advertising, Cookies and Trackers

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Acquisti, A., Gritzalis, S., Lambrinoudakis, C., di Vimercati, S. (2007) Digital Privacy, Theory, Technologies and Practices.
  - Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles.
- Relevant academic journals:
  - Journal of Information Privacy and Security, Taylor & Francis
  - Information and Computer Security, Emerald
  - International Journal of Information Security, Springer
  - Computer Law & Security Review, Elsevier
  - IEEE Security and Privacy Magazine, IEEE
  - Computers and Security, Elsevier
  - Requirements Engineering, Springer
  - IEEE Transactions on Software Engineering, IEEE
  - Security and Communication Networks, Wiley
  - Information Management and Computer Security, Emerald
  - International Journal on Advances in Security, IARIA
  - Journal of Information Security and Applications, Elsevier

3.15.2.1.3 Cybersecurity Governance

COURSE SYLLABUS

- Cybersecurity concepts
- Data Protection, GDPR and DPIA
- The CISO Role
- Cyber Readiness
- ISMS and cybersecurity management
- Cybersecurity Risk Management and Assessment
- Regulation and Compliance
- Cyber Ops and Cyber Warfare

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Jøsang, Audun. Cybersecurity: Technology and Governance. Springer (2024).
  - Tran, Dinh Uy; Jøsang, Audun. Business Language for Information Security. Human Aspects of Information Security and Assurance (HAISA 2023).
  - Tran, Dinh Uy; Jøsang, Audun. Information Security Posture to Organize and Communicate the Information Security Governance Program. European Conference on Management, Leadership & Governance (2022).
  - OECD Digital Economy Papers: New Perspectives on Measuring Cybersecurity, OECD Publishing, June 2024, no. 366.
- Relevant academic journals:
  - Computers & Security (Elsevier)
  - Journal of Cybersecurity (Oxford University Press)
  - Journal of Information Security and Applications (JISA) (Elsevier)
  - IEEE Security & Privacy
  - International Journal of Critical Infrastructure Protection (Elsevier)
  - Information and Computer Security (Emerald)
  - Information Security Journal: A Global Perspective (Taylor & Francis)

3.15.2.1.4 Network Security

COURSE SYLLABUS

- Introduction to Network Security
  - Basic fundamentals and network elements
  - TCP/IP native protocols and main security issues
  - An overview of network-level attacks
- Main network attacks and tools
  - Attacks to confidentiality
  - Attacks to integrity
  - Attacks to availability
  - Other related attacks
- Security protocols in TCP/IP
  - Link-level security
  - Network-level security
  - Transport-level security
  - Application-level security

- Secure network configuration
    - Switches and routers hardening
    - Virtual private networks
    - Firewall and DMZ
    - Detection, prevention, and deception
    - Endpoints hardening (Linux, Windows)

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
    - Computer Networking Hacking: Ultimate Guide To Ethical Hacking, Wireless Network, Cybersecurity With Practical Penetration Test On Kali Linux And System Security Practices (Computer Networking Easy). Ramon Base (autor), ISBN: 978-1083056832, 2019.
    - Implementing and Administering Cisco Solutions: 200-301 CCNA Exam Guide: Begin a successful career in networking with 200-301 CCNA certification. Glen D. Singh (autor), Packt, ISBN: 978-1800208094, 2020.
    - Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Donald A. Tevault (autor), Packt, ISBN: 978-1788620307, 2018.
    - Network Security Strategies. Aditya Mukherjee (autor), Packt, ISBN:9781789806298, 2020.
    - Security Engineering: A Guide to Building Dependable Distributed Systems. Ross Anderson (autor), Wiley, ISBN: 978-1119642787, 2020.
    - pfSense Essentials: The Complete Reference to the pfSense Internet Gateway and Firewall. Jeremy C. Reed (autor), ISBN: 978-1937516048, 2019.
- Relevant academic journals:
    - IEEE Network
    - IEEE Computer Networks
    - IEEE Communications Surveys & Tutorials
    - IEEE Transactions on Secure and Dependable Computing
    - IEEE Transactions on Information Forensics and Security
    - Computers and Security, Elsevier
    - IEEE Security & Privacy
    - ACM Transactions on Privacy and Security, among others
- Relevant academic conferences:
    - BlackHat
    - ESORICS
    - Usenix Security

- ACM Conference on Computer and Communications Security
- IEEE International Conference on Cyber Security and Resilience, among other relevant conferences

3.15.2.1.5 IoT Security

COURSE SYLLABUS

- **IoT Fundamentals:** The course starts with an overview of typical IoT systems, including typical IoT Layers and Architectures, the distinction between IoT and IT, prominent attacks on IoT Devices, and current trends in industrial IoT security.
- **Threat Modelling:** The course then introduces the required background knowledge to model typical IoT threats and assets. This topic comprises terminology, IoT Secure Software Development Life Cycle, ISO 21424, ISO/IEC 18045, Adversary Classification Schemes, Intel Threat Agent Library, Introduction to Asset Taxonomy, OCTAVE, Security Principles and Goals in the context of IoT, STRIDE, MITM attacks, and an introduction to possible Mitigations for typical attacks in the IoT context.
- **Cryptographic primitives in the context of IoT:** As foundation for most defence mechanisms, the course covers the required theoretical background of the cryptographic primitives utilized in typical IoT systems, including Classic Ciphers (e.g. Mono-/Polyalphabetic, Substitution, Transposition), Perfect Forward Secrecy, Symmetric Cryptography (Prominent Examples of Block- and Stream-Ciphers) with focus on AES and it's Operation Modes, Asymmetric Cryptography with focus on RSA, and Digital Signature Schemes (MAC, HMAC, RSA-based).
- **Cryptanalysis:** The course also covers known limitations of the different cryptographic primitives in the context of IoT. This includes attacks such as padding oracle attack, adaptive chosen plain text attacks, integer factorization, among others. In addition, the course looks at some real-life examples of such attacks in different IoT domains including automotive systems.
- **IoT-Specific Communication and Security Patterns**: After having covered the required theoretical background, the course covers the most prominent IoT communication patterns/protocols and highlights them in the context of cybersecurity. This topic area includes coverage of MQTT, XMPP, CoAP, HTTPS, Request/Response Pattern, Asynchronous Messaging, Message Queues, Publisher/Subscriber Pattern, Security Considerations and Limitations of the discussed protocols/patterns, and typical Authorization techniques.
- **Key Exchange Protocols:** the course covers the topic of sharing/exchanging/negotiating cryptographic keys to ensure secure communication among different IoT devices. This will include topics such as Key Transport and Exchange mechanisms and their limitations, Concept of Key Distribution Centres, (Authenticated) Diffie Hellman Key Exchange, Certificates and corresponding PKI

methodologies.

- **Web and Network Security in the context of IoT:** As typical IoT systems are interconnected heavily, the course then covers both theoretical and practical security issues of networked systems. This topic area includes reconnaissance methods using nmap and related tools, Enumeration Techniques in typical web-based IoT devices, Vulnerability Assessment Methodologies, OWASP Top 10 and corresponding common exploit strategies (e.g. SQL injection, XSS) and corresponding toolchains to penetration test such applications.
- **Defence mechanisms**: By then highlighting possible defence mechanisms of typical IoT systems, the course bridges the gap between the discussed security concerns and their practical remediation. This topic area includes Access Control methodologies and patterns for IoT, Authentication mechanisms in the context of typical IoT systems, as well as the limitations and challenges of these concepts.
- **Current Research, Gaps, and Directions:** Throughout the course, attention is given to current scientific developments in both offensive, as well as defensive IoT security. Such literature review sessions are spread throughout the course, aiming to enhance students' critical analysis skills in the context of current research trends.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Adam Shostack, "Threat Modeling: Designing for Security", (https://ieeexplore.ieee.org/book/9932141)
  - ENISA Report, "Good Practices for Security of IoT - Secure Software Development Lifecycle" (https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1)
  - ENISA Report, "Baseline Security Recommendations for IoT" (https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot)
  - Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source Code in C" (https://www.schneier.com/books/applied-cryptography/)
  - Dan Boneh, Victor Shoup, "A Graduate Course in Applied Cryptography" (https://toc.cryptobook.us/book.pdf)
  - Nitesh Dhanjani, "Abusing the Internet of Things" (https://www.oreilly.com/library/view/abusing-the-internet/9781491902899/)
  - Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook, 2nd Edition" (https://www.oreilly.com/library/view/the-web-application/9781118026472/)
- Relevant academic journals/conferences:
  - IEEE Internet of Things Journal
  - ACM Transactions on Internet Technology

- IEEE Transactions on Dependable and Secure Computing

3.15.2.2 2nd Academic Semester

3.15.2.2.1 Study of the Research Area

COURSE SYLLABUS

- Introduction to the Study of Research Field – Objectives, Methodology, and Role. Presentation of the main areas of Cybersecurity.
- Research Map of Cybersecurity: domains, subfields, and international trends (ENISA, NIST, IEEE, ACM).
- Identification of Research Field – Formulation of research problem, purpose, and objectives.
- Systematic Literature Review (PRISMA): sources, methodology, and data organization.
- Critical Evaluation and Comparison of Existing Research Approaches. Identification of knowledge gaps.
- Analysis of Research Publications and Trends – use of bibliometric tools.
- Ethical and Regulatory Frameworks in Cybersecurity Research (ethics, GDPR, Responsible Disclosure).
- Selection and Justification of Research Methodology – quantitative, qualitative, and mixed approaches.
- Cybersecurity Research Data and Tools: datasets, testbeds, and analysis platforms.
- Development of Conceptual and Theoretical Research Frameworks.
- Research Proposal Development – formulation of timeline, objectives, and methods.
- Presentation of Research Proposals – peer review, discussion, and feedback.
- Completion of the Study of Research Field: writing the final Research Field Report and preparation for the main thesis phase.

RECOMMENDED BIBLIOGRAPHY

- Creswell, J. W., & Creswell, J. D. (2023). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE.
- Kitchenham, B., & Charters, S. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. Keele University.
- Oates, B. J. (2006). Researching Information Systems and Computing. SAGE.
- Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2).

- ENISA (2024). Cybersecurity Threat Landscape Report.

3.15.2.2.2 Digital Wellbeing in Cyber-space

COURSE SYLLABUS

- **Introduction to Digital Wellbeing and Cybersecurity:** Explore the key definitions, domains, and interconnections between digital wellbeing and cybersecurity. Examine their growing significance in a hyperconnected world across individual, organizational, and societal contexts.
- **Cybersecurity Basics for Personal Protection:** Gain foundational cybersecurity knowledge including password management, two-factor authentication (2FA), phishing recognition, and digital hygiene for everyday life.
- **Threats to Digital Wellbeing:** Investigate threats such as cyberbullying, online harassment, and digital fatigue. Analyze how these affect mental and emotional wellbeing and learn preventative measures.
- **Social Wellbeing in Cyberspace**: Examine how online harms—cyberbullying, phishing, social engineering—affect social and emotional health. Develop digital literacy and learn how to engage safely and positively in online communities.
- **Digital Addictions and Algorithmic Manipulation:** Analyze the persuasive design features and algorithmic systems used by digital platforms. Explore how they influence user behavior, promote digital dependency, and raise ethical concerns.
- **Mental Health, Burnout, and the Always-On Culture:** Explore the psychological effects of constant connectivity. Learn about technostress, burnout, and the mental health impact of digital overload, along with strategies for resilience and digital self-care.
- **Designing for Security and Wellbeing:** Understand how human-centered UX/UI design can promote both secure systems and digital wellbeing. Examine real-world tech examples and design best practices.
- **Social Media, Misinformation, and Emotional Resilience:** Evaluate the impact of disinformation, online toxicity, and algorithmic filter bubbles. Learn how to strengthen emotional resilience and critical engagement with digital content.
- **Human Factors in Cybersecurity:** Examine the behavioral dimension of cyber risk. Learn how psychological factors, cognitive biases, and user error influence security, and explore tools like nudging and gamification.
- **Ethical Futures:** AI, Surveillance, and the Human Mind: Discuss how AI and surveillance systems affect privacy, autonomy, and mental health. Debate ethical dilemmas related to digital manipulation and data governance.
- **Organizational Cybersecurity and Employee Wellbeing:** Explore the impact of workplace cybersecurity policies on employee mental health and productivity. Study case examples of ethical and balanced approaches to digital safety.

- **Personal Digital Wellbeing Strategy and Reflection:** Reflect on course learnings and develop a personal digital wellbeing and cybersecurity action plan. Discuss future implications and how to implement sustainable digital habits.
- **Intervention Design Workshop:** Apply course concepts by collaboratively designing a practical intervention that integrates cybersecurity and digital wellbeing principles. Peer review and feedback session included.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:

    - Bauman, S., Cross, D., & Walker, J. (Eds.). (2013). Principles of cyberbullying research: Definitions, measures, and methodology. Routledge.
    - Brewer, J. (2017). The craving mind: From cigarettes to smartphones to love—Why we get hooked and how we can break bad habits. Yale University Press.
    - Büchi, M. (2022). Digital well-being: Conceptualizations, implications, and open questions. New Media & Society, 24(2), 337–355.
    - Cecchinato, M. E., Rooksby, J., Hiniker, A., Munson, S., Lukoff, K., Ciolfi, L., ... & Harrison, D. (2019, May). Designing for digital wellbeing: A research & practice agenda. In Extended abstracts of the 2019 CHI conference on human factors in computing systems (pp. 1–8). ACM.
    - Crouch, A. (2017). The tech-wise family: Everyday steps for putting technology in its proper place. Baker Books.
    - Filep, S., Kondja, A., Wong, C. C. K., Weber, K., Moyle, B. D., & Skavronskaya, L. (2023). The role of technology in users' wellbeing: Conceptualizing digital wellbeing in hospitality and future research directions. Journal of Sustainable Tourism, 31(5), 583–601.
    - Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. Archives of Suicide Research, 14(3), 206–221.
    - Hinduja, S., & Patchin, J. W. (2024). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (3rd ed.). Corwin Press.
    - Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137.
    - Krause, C. (2024). Digital wellbeing: Empowering connection with wonder and imagination in the age of AI. Wiley.
    - Monge Roffarello, A., & De Russis, L. (2019, May). The race towards digital wellbeing: Issues and opportunities. In Proceedings of the 2019 CHI conference on human factors in computing systems (pp. 1–14). ACM.
    - Patchin, J. W., & Hinduja, S. (2014). Words wound: Delete cyberbullying and make kindness go viral. Free Spirit Publishing.

- Patchin, J. W., & Hinduja, S. (2016). Bullying today: Bullet points and best practices. Corwin Press.
- Regehr, K. (2025). Smartphone nation: Digital addiction and how to break free. Bloomsbury Academic.
- Roffarello, A. M., & De Russis, L. (2023). Achieving digital wellbeing through digital self-control tools: A systematic review and meta-analysis. ACM Transactions on Computer-Human Interaction, 30(4), 1–66.
- Schlyakhto, E., Ilin, I., Devezas, T., Correia Leitão, J. C., & Cubico, S. (2024). Innovations for healthcare and wellbeing: Digital technologies, ecosystems and entrepreneurship. Springer.
- Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, 29(1), 26–32.
- Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behavior, 26(3), 277–287.
- Turkle, S. (2015). Reclaiming conversation: The power of talk in a digital age. Penguin Press.
- Vanden Abeele, M. M. P. (2021). Digital wellbeing as a dynamic construct. Communication Theory, 31(4), 932–955.
- Willard, N. (2007). Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Research Press.
- Wong, B. L. H., Maaß, L., Vodden, A., van Kessel, R., Sorbello, S., Buttigieg, S. C., & Odone, A. (2022). From digital health to digital well-being: A systematic scoping review. Journal of Medical Internet Research, 24, Article e33787.

- Relevant academic journals:
  - **Digital Wellbeing, Cyberpsychology & Human Behavior**
    - **Journal of Cybersecurity**
      - Focus: Cybersecurity policy, technical, and human dimensions
      - Publisher: Oxford University Press
      - https://academic.oup.com/cybersecurity
    - **Cyberpsychology: Journal of Psychosocial Research on Cyberspace**
      - Focus: Online behavior, cyberbullying, digital wellbeing, and psychosocial research
      - Publisher: Masaryk University
      - https://cyberpsychology.eu/
    - **Computers in Human Behavior**
      - Focus: Human interaction with digital technologies, including mental health and screen time

        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/computers-in-human-behavior
    - **Journal of Medical Internet Research (JMIR)**
        - Focus: Digital health, eHealth, digital wellbeing
        - Publisher: JMIR Publications
        - https://www.jmir.org/
    - **Communication Theory**
        - Focus: Theoretical and empirical research in communication, including digital wellbeing
        - Publisher: Oxford University Press
        - https://academic.oup.com/ct
    - **Journal of Computer-Mediated Communication (JCMC)**
        - Focus: Social and interpersonal communication in digital media
        - Publisher: Oxford University Press
        - https://academic.oup.com/jcmc
    - **New Media & Society**
        - Focus: Socio-cultural impacts of new media and technology, including wellbeing
        - Publisher: SAGE
        - https://journals.sagepub.com/home/nms
    - **Technology in Society**
        - Focus: Social impacts of emerging technologies, ethics, and behavior
        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/technology-in-society
    - **Information, Communication & Society**
        - Focus: Intersection of technology, communication, and society
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/rics20
- **Human–Computer Interaction (HCI) & UX**
    - **ACM Transactions on Computer-Human Interaction (TOCHI)**
        - Focus: Interaction design, user experience, digital self-control tools
        - Publisher: ACM
        - https://dl.acm.org/journal/tochi
    - **International Journal of Human-Computer Studies**
        - Focus: HCI, UX design, and digital behavior

        - Publisher: Elsevier
        - https://www.sciencedirect.com/journal/international-journal-of-human-computer-studies
    - **Behaviour & Information Technology**
        - Focus: Human interaction with technology and design for wellbeing
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/tbit20
- **Psychological and Media Effects**
    - **Media Psychology**
        - Focus: Media influence on emotions, cognition, addiction, and wellbeing
        - Publisher: Taylor & Francis
        - https://www.tandfonline.com/journals/hmep20

3.15.2.2.3 Offensive Security

COURSE SYLLABUS

- **Open Source INTelligence:** collecting general information about the target, google hacking, social media search, archive search, collecting technical information, domain and domain owner data search, IP address related search, network range owner identification, network range enumeration
- **Network reconnaissance:** mapping the network with different techniques, nmap and hping usage with different options
- **Get in touch with services:** Identifying and attacking different services, finding information disclosure and default settings, brute-force, understanding exploits in general, service related unique exploitation techniques
- **Web hacking:** Information disclosure and defaults, brute-force, client side manipulation and tampering, XSS, CSRF, server side techniques, session related exploitations, file inclusions, SQLi, XPathi, SSTI, XXE, etc.
- **Binary exploitation:** understanding binaries, CPU architectures and binaries in general, virtual address spaces and layouts, debugging, understanding the stack, stack overflow, return to libc, return oriented programming exploitations, heap related vulnerabilities, use after free and heap spraying
- **Social Engineering:** understanding the human behavior, phishing techniques, other social engineering techniques
- **Internal Network Hacking:** getting access to internal networks, Microsoft network related protocols and exploitation, man in the middle techniques, ARP poisoning

- **Ethical hacking and cryptography:** password cracking techniques
- **Wireless Security:** WEP and WPA2, capturing the wifi handshake, cracking

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Lecture slides will provide up-to-date bibliography
- Relevant academic journals:
  - Journal of Cybersecurity (Oxford University Press)
  - IEEE Security & Privacy
  - Cybersecurity (SpringerOpen)

3.15.2.2.4 Forensics

COURSE SYLLABUS

- **Introduction to Digital Forensics:** Chain of custody, evidence lifecycle, forensic roles
- **Data Acquisition, File Data, and Metadata:** Disk acquisition techniques, filesystem analysis, metadata and artifact extraction, hashing, etc.
- **Windows Native Artifacts 1:** Windows Artifacts: Prefetch, Registry, Event Logs, LNK, Jumplist, etc.
- **Windows Native Artifacts 2:** Windows Artifacts: Prefetch, Registry, Event Logs, LNK, Jumplist, etc.
- **Web Browser Artifacts:** Chrome and Firefox Artifacts: History, Downloads, Bookmarks, etc.
- **Advanced Forensic Concepts:** Cloud, Mobile, IoT and other advanced concepts
- **SOC Fundamentals:** SOC structure, L1–L3 responsibilities, tooling overview
- **SIEM Operations and Alert Triage:** SIEM architecture, log ingestion, initial alert handling
- **Incident Response 1:** IR lifecycle, Collection and Analysis of Triage Image
- **Incident Response 2:** Memory Acquisition and Analysis
- **Threat Intelligence and CTI:** CTI lifecycle, MISP, threat actor profiling
- **Threat Hunting and Detection Engineering:** Hypothesis-driven hunting, ATT&CK mapping, detection rule development
- **AI in Cyberdefence and SOC Automation:** AI for alert triage, phishing detection, etc.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:

- William Oettinger, Learn Computer Forensics – 2nd edition: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence , Second Edition (2022)
- Anson, S. (2020). Applied incident response. Wiley.
- Murdoch, D. (2019). Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02): A condensed guide for the security operations team and threat hunter. Independently published.

- Relevant academic journals:
  - Digital Investigation (Elsevier)
  - Journal of Cybersecurity (Oxford University Press)
  - Journal of Forensics Sciences (Wiley)
  - IEEE Transactions on Information Forensics and Security
  - Computers & Security (Elsevier)
- Related conferences
  - DFRWS (Digital Forensics Research Workshop)
  - SANS DFIR & Blue Team Summits
  - Black Hat SECTOR

3.15.2.2.5 Secure Autonomous Systems

COURSE SYLLABUS

- **Fundamental Material on autonomous systems:** The course starts by discussing the theoretical background of typical autonomous systems, including typical architectures and functional blocks of autonomous vehicles and drones with focus on the layered architecture, simulation environments for End-to-End testing of autonomous systems, notable examples of real-world attacks against autonomous vehicles, and the current state of security research in this domain.
- **Threat Modelling:** As basis for further discussion, the course then covers important threat- and asset classification methodologies for automotive systems (e.g. EVITA), as well as their application to autonomous systems.
- **Camera Sensor Processing Pipelines:** The course then inspects the typically utilized camera sensor technologies and their underlying security context. This topic area includes the typically performed data (pre-)processing steps, the underlying sensor data processing pipeline between sensor and perception layer, typical perception layer building blocks, security implications of the processing pipeline, and the current state of security research in the context of camera-based sensing systems.
- **Lidar Sensor Processing Pipelines:** The course then inspects LiDAR sensor processing pipelines as a second type of important sensing technology of autonomous vehicles. Similar to the camera-based topic area, this topic area introduces the typical

sensor data (pre-)processing steps, the typically utilized sensor data pipeline between sensor and perception layer, typical perception layer building blocks, as well as the underlying security implications and current offensive and defensive research topics in autonomous LidAR applications.

- **Sensor Fusion, Collaborative Perception and Real-Time Systems:** After establishing the theoretical background for both LiDAR- and Camera-based systems, the course then covers typical sensor fusion approaches, in which these two sensing systems are combined. Next to an overview of such sensor fusion / multi-modal sensing approaches, current research directions and security considerations are discussed. Additionally, typical applications of multi-system collaborative perception approaches are discussed, and current research and security implications highlighted. As autonomous systems typically utilize real-time methodologies, the theoretical background, as well as important attacks and defences for such real-time systems are covered.
- **Wired and wireless communication in the context of autonomous vehicles:** The course then highlights the security context of typically utilized wired and wireless communication architectures and protocols found in autonomous systems. To give all students, independent of their exact technical background, the possibility of researching such communication systems as typically found in autonomous systems and their environment, the course offers an introduction into the required RF physics and handling of Software Defined Radios (SDR) using open-source toolkits like GNUradio. Similarly, the theoretical background of wired in-vehicle communication is covered (e.g. CAN and LIN), and the security implications of the typically utilized communication systems and protocols, as well as current research trends are highlighted.
- **Reactive and Preventative Security:** To highlight the typically proposed defensive measures intended to protect the discussed autonomous system weaknesses, the course covers both reactive (e.g. automotive IDS) and preventative (e.g. testing-based approaches like simulation-based fuzzing) defensive measures. Current trends in research are highlighted, and the current gaps in the proposed countermeasures are critically discussed.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Bruce Schneier, "Applied Cryptography Protocols, Algorithms, and Source Code in C" (https://www.schneier.com/books/applied-cryptography/)
  - Dr. Charlie Miller, Chris Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle" (https://illmatics.com/Remote%20Car%20Hacking.pdf)
  - Craig Smith, "The Car Hacker's Handbook" (https://nostarch.com/carhacking)
- Relevant academic journals/conferences:

- USENIX Symposium on Vehicle Security and Privacy (VehicleSec)
- Network and Distributed System Security Symposium (NDSS)
- ACM Conference on Embedded Networked Sensor Systems (SenSys)

3.15.2.2.6 Cybersecurity: Attack, Defence, and Operational Practice

COURSE SYLLABUS

- **Introduction:** Introduces the cybersecurity landscape, common threat actors, and the ethical foundations of hacking and defence. Students explore major breaches and set up a virtual lab environment for hands-on practice.
- **Reconnaissance & OSINT:** Covers passive and active information gathering techniques used by attackers. Students learn how to use OSINT tools to perform footprinting and gather intelligence about potential targets.
- **Scanning & Enumeration:** Explores the techniques used to scan networks and enumerate services, users, and system information. Hands-on labs use tools like Nmap to map attack surfaces and discover vulnerabilities.
- **Exploitation Techniques:** Focuses on exploiting known vulnerabilities in web applications, systems, and services. Students gain experience using frameworks like Metasploit in a controlled environment.
- **Post-Exploitation & Lateral Movement:** Examines methods attackers use after gaining access, such as privilege escalation, persistence, and moving through a network. Students perform post-exploitation tasks in simulated scenarios.
- **Defence Mechanisms:** Introduces defence-in-depth principles and key defensive technologies like firewalls, antivirus, and IDS/IPS. Students learn how to configure security controls on hosts and networks.
- **Security Monitoring & Logging:** Covers how to detect attacks through monitoring and log analysis. Students work with SIEM tools to identify indicators of compromise and correlate events.
- **Incident Response:** Explains the incident response lifecycle: preparation, detection, containment, eradication, recovery, and lessons learned.
- **Threat Intelligence:** Explores types of cyber threat intelligence (CTI), threat actor profiling, and intelligence feeds. Students learn how to produce and apply intelligence to enhance detection and defence.
- **Security Operations Centers (SOC):** Introduces the function, tools, and processes of a SOC. Students simulate working in a SOC environment, handling alerts, performing triage, and documenting responses.
- **Malware Analysis & Reverse Engineering:** Covers basic malware types, static and dynamic analysis, and sandboxing. Students safely examine malware samples to understand behavior and indicators.

- **Identity, Access Management & Zero Trust Architectures:** Focuses on the principles of secure authentication, authorization, identity governance, and Zero Trust models. Explores multifactor authentication (MFA), SSO, and access control weaknesses.
- **Capstone & Assessment:** Students apply their knowledge in a final presentation or practical demonstration based on a real-world attack-defence or operational security scenario.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Alsmadi, I. (2023). The NICE cyber security framework: Cyber security intelligence and analytics. Springer. https://doi.org/10.1007/978-3-031-21651-0
  - Diogenes, Y., & Ozkaya, E. (2022). Cybersecurity – Attack and defense strategies: Red and blue team tactics for security professionals (3rd ed.). Packt Publishing.
- Relevant academic journals:
  - Journal of Cybersecurity (Oxford University Press)
  - IEEE Security & Privacy
  - International Journal of Critical Infrastructure Protection (Elsevier)
  - Cybersecurity (SpringerOpen)

3.15.2.2.7 Cybersecurity in Industrial Scenarios

COURSE SYLLABUS

- Industrial scenarios and smart technologies
  - Industrial scenarios
  - CPS-IIoT and other technologies in industrial scenarios
  - Industrial communication protocols
- Cybersecurity threats for industrial scenarios
  - Main cybersecurity issues in industrial scenarios
  - Threats taxonomy and real cases
- Essential cybersecurity capabilities for industrial scenarios
  - Zero-trust and defence in-depth principles
  - Regulatory frameworks, standards and recommendations
  - Industrial perimeter security
  - Secure connection and accessibility
- Advanced cybersecurity capabilities for industrial scenarios
  - Proactive and active defence
  - Continue monitoring and assessment
  - Simulation for protection, training, and testing

- Trust and privacy

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - Shinde, A., Lokegaonkar, B. (2024). Industrial Cybersecurity: A Practical Approach to OT Protection. (n.p.): CyberAuthor.
  - Ackerman, P. (2021). Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment. Alemanya: Packt Publishing.
  - Shinde, A., Lokegaonkar, B. (2024). Industrial Cybersecurity: A Practical Approach to OT Protection. (n.p.): CyberAuthor.
  - Knapp, E. D. (2024). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Estats Units d'Amèrica: Syngress
- Relevant academic journals:
  - IEEE Transactions on Industrial Informatics
  - IEEE Transactions on Industrial Cyber-Physical Systems
  - ACM Transactions on Cyber-Physical Systems
  - IEEE Communications Surveys & Tutorials
  - IEEE Transactions on Secure and Dependable Computing
  - IEEE Transactions on Information Forensics and Security
  - Computers and Security, Elsevier
  - IEEE Security & Privacy
  - ACM Transactions on Privacy and Security, among others
- Relevant academic conferences:
  - BlackHat
  - ESORICS
  - Usenix Security
  - ACM Conference on Computer and Communications Security
  - IEEE International Conference on Cyber Security and Resilience, among other relevant conferences

3.15.2.2.8 Cybersecurity in the Political Domain: Internal and External Dimensions)

COURSE SYLLABUS

- **Introduction to Cyber Threats, Cyber Resilience, and Cyber Politics**: This opening week lays the foundation by introducing key concepts of cybersecurity, cyber resilience, and cyber politics in global affairs. Students will explore how cyber threats have evolved into political issues both internally and externally.

- **Cyber Threats to Democracy – Institutions, Disinformation, and Social Impact:** This week examines how cyber threats undermine democratic institutions and civic processes. Topics include election interference, disinformation operations, and online polarization. Through case studies, students assess the erosion of public trust and explore how digital literacy, civic tech, and regulatory interventions can strengthen democratic resilience.
- **State and Non-State Actors in Cyberspace:** Students will analyze the range of actors active in cyberspace—nation-states, proxy groups, cybercriminals, hacktivists, and private cybersecurity contractors. The session focuses on motivation, tactics, and the complexities of attribution, as well as the strategic use of non-state actors in hybrid conflicts.
- **Cyber Threats to Social and Cultural Dimensions:** This session investigates how cyber threats affect human behavior, public trust, and digital culture. Students assess cross-cultural cybersecurity perceptions, and analyze issues like social engineering, online manipulation, and the psychological effects of cybercrime and disinformation.
- **Cybersecurity in World Politics – Geopolitics and National Strategies:** This week focuses on how cybersecurity has become a major factor in global politics and geopolitics, significantly impacting international relations and national security strategies. It's seen as a tool for achieving national interests, and cybersecurity threats are increasingly seen as a diplomatic and political issue.
- **Cybersecurity and International Relations Theories:** This week, students will apply classical and contemporary theories of International Relations (IR)—such as realism, liberalism, constructivism, and critical theories—to analyze cyber-related challenges. Through theoretical lenses, students will examine how states and non-state actors behave in cyberspace, how power and cooperation manifest in the digital realm, and how ideational factors influence cybersecurity discourse and policy. The week emphasizes the value of theory in understanding strategic behavior, norm development, and the global governance of cyberspace.
- **Impact of Cyber Threats and Attacks (Part I) – Military and Security Dimensions:** This week explores the impact of cyber threats and attacks on the military and national security domains. Students will examine the use of cyberattacks for espionage, cyber warfare, terrorism, and the disruption of defence operations. The session analyzes vulnerabilities in military systems, intelligence networks, and command-and-control infrastructures. Key topics include the risk of escalation, the blurring of civilian and military targets, and the role of cyber capabilities in hybrid warfare and strategic deterrence.
- **Impact of Cyber Threats and Attacks (Part II) – Diplomatic and Political Dimensions:** Building on the military-security focus of Week 7, this session examines how cyber threats and attacks impact diplomacy and political relations between states. Students will explore how high-profile cyber incidents can erode interstate trust, strain alliances, and complicate traditional diplomatic efforts. The session

addresses the challenges of cyber attribution, including technical uncertainty and political consequences, and considers how states respond through sanctions, public attributions, or legal indictments. Particular emphasis is placed on the difficulties of maintaining dialogue during and after cyber crises, the use of crisis communication mechanisms, and the role of international norms and law in shaping state behavior. Students will also analyze the impact of hybrid operations that blend cyberattacks with disinformation campaigns, further complicating diplomatic responses and conflict resolution.

- **Impact of Cyber Threats and Attacks (Part III) – Economic Dimensions:** This session addresses the economic impact of cyber threats, focusing on disruptions to financial systems, theft of intellectual property, and attacks on critical infrastructure. Students will examine how cyber incidents such as ransomware attacks, corporate espionage, and supply chain compromises can lead to significant financial losses, undermine investor confidence, and threaten national economic stability. The session also explores the long-term implications of persistent cyber threats on economic resilience, competitiveness, and the digital transformation of critical sectors.
- **International Law and Ethics in Cyberspace:** This week explores the legal and ethical dimensions of state and non-state behavior in cyberspace. Students will examine key legal frameworks, including the Tallinn Manual and the Budapest Convention, and critically engage with core principles such as sovereignty, due diligence, and proportionality in the context of cyber operations. Ethical considerations—ranging from privacy and surveillance to state repression and digital rights—will be discussed, encouraging students to assess the limitations and possibilities of current legal instruments and norm-building efforts in governing cyberspace.
- **Emerging Technologies, AI, and the Future of Cyber Conflict:** This forward-looking session investigates the transformative impact of emerging technologies on the cyber threat landscape. Students will explore how artificial intelligence, quantum computing, and autonomous systems are reshaping both offensive and defensive cyber capabilities. Key topics include AI-enabled disinformation, automated cyber operations, and the ethical dilemmas posed by algorithmic decision-making in warfare and surveillance. The session emphasizes the growing complexity of threat prediction, attribution, and response in the face of rapid technological advancement.
- **Strategic Responses and Capacity Building for Cyber Resilience:** This week focuses on strategies for enhancing cyber resilience at national and international levels. Students will analyze the roles of public-private partnerships, cybersecurity education and training, critical infrastructure protection, and capacity-building initiatives in strengthening societal resilience to cyber threats. Emphasis is placed on cross-sector collaboration, institutional preparedness, and policy coherence across technical, legal, and political domains.
- **Cyber Crisis Simulation – Strategic Response and Diplomacy in Action:** In this capstone simulation, students will apply their knowledge in a dynamic, real-time

cyber crisis scenario involving a multi-stage attack on critical infrastructure. Working in role-specific teams—representing governments, international organizations, media outlets, and private technology firms—students will develop and implement coordinated responses involving decision-making, legal and ethical analysis, public communication, and diplomatic negotiation. The simulation concludes with a structured debrief, highlighting lessons learned, strategic missteps, and the inherent complexity of cyber governance in high-pressure environments.

RECOMMENDED BIBLIOGRAPHY

- Suggested bibliography:
  - **Books**
    - Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
    - Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.
    - Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
    - Nye, J. S. (2011). The future of power. PublicAffairs.
    - Rid, T. (2013). Cyber war will not take place. Oxford University Press.
    - Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
    - Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. PublicAffairs.
    - Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
    - Valeriano, B., & Maness, R. C. (2015). Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press.
    - Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.
  - **Journal Articles**
    - Bradshaw, S., & Howard, P. N. (2019). The global disinformation order. Oxford Internet Institute Working Paper, 2019(3).
    - Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.
    - Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. American Journal of International Law, 110(3), 425–479.
    - Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. International Security, 38(2), 7–40.

    - Taddeo, M. (2018). The Limits of Deterrence Theory in Cyberspace. Philosophy & Technology, 31(2)
- Relevant academic journals:
  - **International Security**
    - Published by MIT Press, this journal features foundational work on cyber conflict, deterrence, and cyber-enabled statecraft.
    - International Security. (n.d.). MIT Press. https://direct.mit.edu/isec
  - **Journal of Strategic Studies**
    - Covers strategic theory and national security, including cyberwarfare and defense planning.
    - Journal of Strategic Studies. (n.d.). Taylor & Francis. https://www.tandfonline.com/journals/fjss20
  - **European Journal of International Security**
    - Explores international security issues through critical, constructivist, and strategic lenses—including cyberspace as a security domain.
    - European Journal of International Security. (n.d.). Cambridge University Press. https://www.cambridge.org/core/journals/european-journal-of-international-security
  - **Security Dialogue**
    - A key journal in critical security studies, publishing on the politics and discourse of cybersecurity, digital surveillance, and hybrid threats.
    - Security Dialogue. (n.d.). SAGE Publications. https://journals.sagepub.com/home/sdi
  - **International Affairs**
    - One of the oldest IR journals, covering cyber diplomacy, global norms, and state responses to digital threats.
    - International Affairs. (n.d.). Chatham House / Oxford University Press. https://academic.oup.com/ia
  - **Review of International Studies**
    - Publishes theoretical and empirical work on global politics, including cybersecurity as an emerging topic in global governance.
    - Review of International Studies. (n.d.). Cambridge University Press. https://www.cambridge.org/core/journals/review-of-international-studies
  - **Foreign Policy Analysis**
    - Focuses on decision-making, strategic culture, and how state actors navigate issues like cyber threats.
    - Foreign Policy Analysis. (n.d.). Oxford University Press. https://academic.oup.com/fpa
  - **Global Studies Quarterly**
    - Publishes cutting-edge work on digital geopolitics, cyber cooperation, and IR theory in the age of AI and big data.

    - Global Studies Quarterly. (n.d.). International Studies Association. https://academic.oup.com/isagsq
- **Politics & Governance**
    - Open-access journal that frequently publishes thematic issues on digital authoritarianism, cyber diplomacy, and governance of emerging technologies.
    - Politics & Governance. (n.d.). Cogitatio Press. https://www.cogitatiopress.com/politicsandgovernance
- **Contemporary Security Policy**
    - Publishes empirical and conceptual studies on international security, including cyber strategy, resilience, and cyber-enabled warfare.
    - Contemporary Security Policy. (n.d.). Taylor & Francis. https://www.tandfonline.com/journals/fcsp20

3.15.2.3 3rd Academic Semester

3.15.2.3.1 Master Thesis

Framework for the Preparation of the Thesis

The Master Thesis shall, as a rule, be undertaken individually or in groups by each postgraduate student, under the supervision of a faculty member of the M.Sc. program (Supervisor), in accordance with the provisions of applicable legislation, and shall address a subject that falls within the scientific scope of the program.

The Thesis must be based on a rigorous research methodology, include primary data analysis, the development or evaluation of research models, algorithms, or security frameworks, and aim for a clear scientific contribution to the field of Cybersecurity.

The Master Thesis may address theoretical or applied topics. It may also be undertaken in collaboration with a private or public body that operates in, or has an interest in, fields related to the subject matter of the program, in accordance with the provisions of applicable legislation.

Evaluation and Grading Criteria

The assessment of the thesis is based on the quality of the selection of bibliographic sources, the scientific accuracy in the analysis of existing knowledge, the depth of engagement with the field, the breadth of topic coverage, the precision of description, the coherence and clarity of argumentation, the extent of research contribution and generation of new knowledge in the scientific field, the overall scientific maturity of the work, compliance with formatting and content requirements as set out in the relevant guidelines, as well as the completeness and maturity demonstrated in the oral

presentation. Assessment will also consider the effective use of the allocated time and the scientifically sound responses of the student to questions posed by the Examination Committee.

Further details regarding the procedures to be followed and the overall framework for application submission, supervision during preparation, writing, presentation, and formal evaluation are set out in Appendix 7: Master Thesis Preparation Regulation).

3.16 Learning Outcomes

3.16.1 Knowledge

Within the scope of the M.Sc., students acquire advanced knowledge in the following core areas:

- **Research Methodology and Scientific Thinking**
  - Students gain an in-depth understanding of the concept, objectives, and role of research in cybersecurity technologies, data protection, and the governance of related environments.
  - They distinguish and comprehend the methodological approaches of scientific research (quantitative, qualitative, and mixed methods) and the processes for their application.
  - They understand the structure and key components of a research problem, as well as the procedures for data collection, processing, and validation.
  - They acquire knowledge of the basic principles of statistical analysis, the evaluation of research results, and the importance of data reliability.
  - They recognize the role of literature review, are familiar with techniques for identifying and documenting sources, and are able to identify research gaps.
  - They understand the institutional, ethical, and regulatory framework governing the conduct of research.
  - They comprehend the principles of academic writing, evidence-based presentation, and the preparation of research proposals
- **Specialization and Applied Knowledge.** Through elective courses, graduates acquire specialized knowledge in specific thematic areas such as:
  - Regulatory and legal frameworks for data protection and governance
  - Privacy protection and privacy-enhancing technologies
  - Analysis of ethical and social issues arising from modern technologies
  - Cybersecurity, network security, cyber resilience, and risk management
  - Advanced technologies and artificial intelligence in data protection and information security
- **Production of New Knowledge and Research Autonomy**
  - They develop the ability to design and conduct original research in the field of Cybersecurity.

- They cultivate critical and creative thinking for addressing complex research problems.
- They understand the principles of scientific documentation and dissemination of research results through publications, presentations, and conference contributions.
- They are able to contribute to the advancement of scientific knowledge and to operate in research, academic, or industrial environments.

3.16.2 Skills

The programme is structured to integrate contemporary interdisciplinary knowledge with frameworks for its effective and efficient application. Its aim is to equip postgraduate students with skills for independent research, scientific documentation, and applied analysis, thereby enhancing their professional prospects in research institutions. Upon completion of the programme, postgraduate students are expected to be able to:

- Identify, analyze, and evaluate relevant literature, critically synthesizing findings and recognizing trends, challenges, and research gaps.
- Formulate appropriate research questions, hypotheses, and objectives based on evidence-based analysis.
- Select, justify, and apply appropriate research methodologies (quantitative, qualitative, or mixed methods) relevant to their research field.
- Design and develop coherent research proposals with clear theoretical and methodological frameworks.
- Apply techniques for data collection, analysis, thematic analysis, and data visualization.
- Recognize the stages and types of the research process and organize documentation and referencing tools.
- Collect, evaluate, and document digital data while ensuring the reliability and validity of information.
- Write and format scientific texts and present and defend their research proposals before academic audiences.
- Develop the ability to formulate comprehensive research proposals and deliver structured presentations.
- Apply ethical principles in conducting research studies and ensure compliance with institutional and ethical standards.

3.16.3 Competences

Postgraduate students develop competences that enable them to become independent researchers capable of applying advanced technologies and leading strategic processes in Cybersecurity and Data Protection. In particular, graduates will be able to:

- Link the research process with practical problems in the field and define the scope of research.

- Design and implement comprehensive research protocols, selecting appropriate tools and ensuring data quality.
- Analyze quantitative and qualitative data and derive evidence-based conclusions.
- Develop a responsible research attitude and apply ethical principles and standards of academic integrity.
- Collaborate effectively with supervisors and research teams, communicate research results to specialist audiences, and connect theoretical findings with practical applications in the field of Cybersecurity.
- Develop and document new research knowledge frameworks using innovative methodologies.
- Work autonomously and design original research projects.
- Contribute to the production of new knowledge in academic, research, or industrial environments by utilizing advanced technologies and methodologies.

3.17 Preparation of assignments

Postgraduate students, in accordance with the provisions set out in the Regulations and the Study Guide of the M.Sc., may be required to prepare assignments as part of the course assessment process. For further information regarding the preparation of assignments, please refer to Appendix 6: Regulations for the Preparation of Assignments

3.18 Preparation of the Master Thesis through Erasmus

Postgraduate students have the option of preparing their thesis under the LLP Erasmus programme, either in European Union member states or in third countries: (a) in collaboration with universities or research institutes; or (b) through the Erasmus Internship programme in private or public enterprises and organizations. For further information regarding the preparation of the Master Thesis, please refer to Appendix 7: Master Thesis Preparation Regulation

3.19 Digital Services

3.19.1 Digital Services of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»

The M.Sc. «Advanced Cybersecurity Technologies and Governance by Research» offers to its postgraduate students a set of electronic services for supporting their academic activities.

3.19.1.1 M.Sc., Department of Digital Systems, and University of Piraeus websites

Central point of information and announcement postings will be the M.Sc. website (https://cybersecgov-res.ds.unipi.gr/en/home/), the Department of Digital Systems

website (https://www.ds.unipi.gr/en/) and the University of Piraeus website (https://www.unipi.gr/en/).

3.19.1.2 Course Management System «LEFKIPPOS» (Open eClass)

The program provides its students with the asynchronous Open eClass platform «Lefkippos» via the address https://lefkippos.ds.unipi.gr/index.php?localize=en, acting as a comprehensive Electronic Course Management System. It follows the philosophy of open-source software and supports asynchronous e-learning without any restrictions or limitations. Access to the platform does not require any specialized technical knowledge and is possible through a web browser. Students must log in to «Lefkippos» exclusively through the Central Authentication Service (CAS). To log in via CAS, students must first activate their institutional account through URegister (https://www.unipi.gr/en/uregister-2/).

After their first successful login to the system via CAS, all students must update (or confirm) in their account profile: the category (M.Sc. Program/M.Sc. Specialization) they belong to, their student identification number, and their phone number. In addition, they must ensure that the «E-mail» field is filled in with their institutional unipi e-mail address and that this email is verified on the «Lefkippos» platform.
For information and support, the students may contact the platform administrators via the «Contact» option.

3.19.1.3 Virtual Campus

The M.Sc. Program, in addition to the distance-learning infrastructures of the Institution, will make use of the pan-European digital and inter-university campus developed within the framework of the European project EU-iNSPIRE, in which it participates and coordinates. This Virtual Campus focuses on the development of advanced knowledge and skills for cybersecurity and constitutes the primary operational environment through which both the educational activities and the training activities associated with the M.Sc. Program will be delivered.

The Virtual Campus operates as a unified, flexible, and accessible e-learning environment, that integrates different digital modules and technologies, can function in combination with the Institution's existing digital environments, and is capable of supporting distance education, virtual mobility, and collaboration among multiple partners at a European level.

The Virtual Campus:

- enables structured and traceable onboarding of learners,
- supports modular, skills-oriented learning delivery aligned with industry needs,

- ensures accessibility and inclusiveness across linguistic, social, and physical dimensions,
- and generates verifiable evidence of participation, assessment, and certification in line with EU funding requirements

Particular emphasis is placed on skills development, including hands-on, practice-oriented learning components, competence assessment, and structured certification pathways. As a result, the Virtual Campus supports not only the delivery of content, but also the measurable acquisition and evaluation of skills.

In addition, it supports selection and enrolment processes that comply with principles of gender equality and social inclusion, as well as with security, privacy, and data-protection guidelines.

Finally, the general obligations for record-retention, substantiation, and reporting are fulfilled, meaning that the Virtual Campus serves as a reliable source of evidence for the implementation and outcomes of the educational process.

Each stage is supported by a designated platform:

- **DreamApply** governs admissions and onboarding (DreamApply Knowledge Base),
- **LearnWorlds** governs learning delivery, assessment, and certification (https://www.learnworlds.com/),
- **Weglot** ensures multilingual access across the environment.
- **accessiBe** ensures accessibility and inclusive interaction.

3.19.1.4 Master's Program Electronic Application Submission System «ARISTYLLOS»

The Program provides an electronic system for the submission of applications by canditate students, namely «Aristyllos», available at https://aristyllos.ds.unipi.gr/web/. Registration in the «Aristyllos» system is done through the home page. After activating the account and successfully logging into the system, the candidate may submit an application for admission to the M.Sc..

3.19.1.5 Student information & academic evaluation portal for the M.Sc. «SIS-PORTAL»

The monitoring of academic progress is carried out through the Student Information Portal (electronic secretariat service) at the address: https://sis-portal.unipi.gr/.

Through that portal, students can:

- be informed about the courses of the curriculum,
- be informed about the teachers and the proposed textbooks,
- see the announcements issued by the Secretariat and the teachers,
- see the grades in the courses they have been examined in,
- submit electronically the course selections of each semester,
- receive immediately and in electronic form proof of enrollment,
- submit special certificate applications

Access to the portal is granted through each student's personal account. Furthermore, through the same portal the students can evaluate each course, each instructor, and the M.Sc. facilities, by confidentially completing evaluation questionnaires.

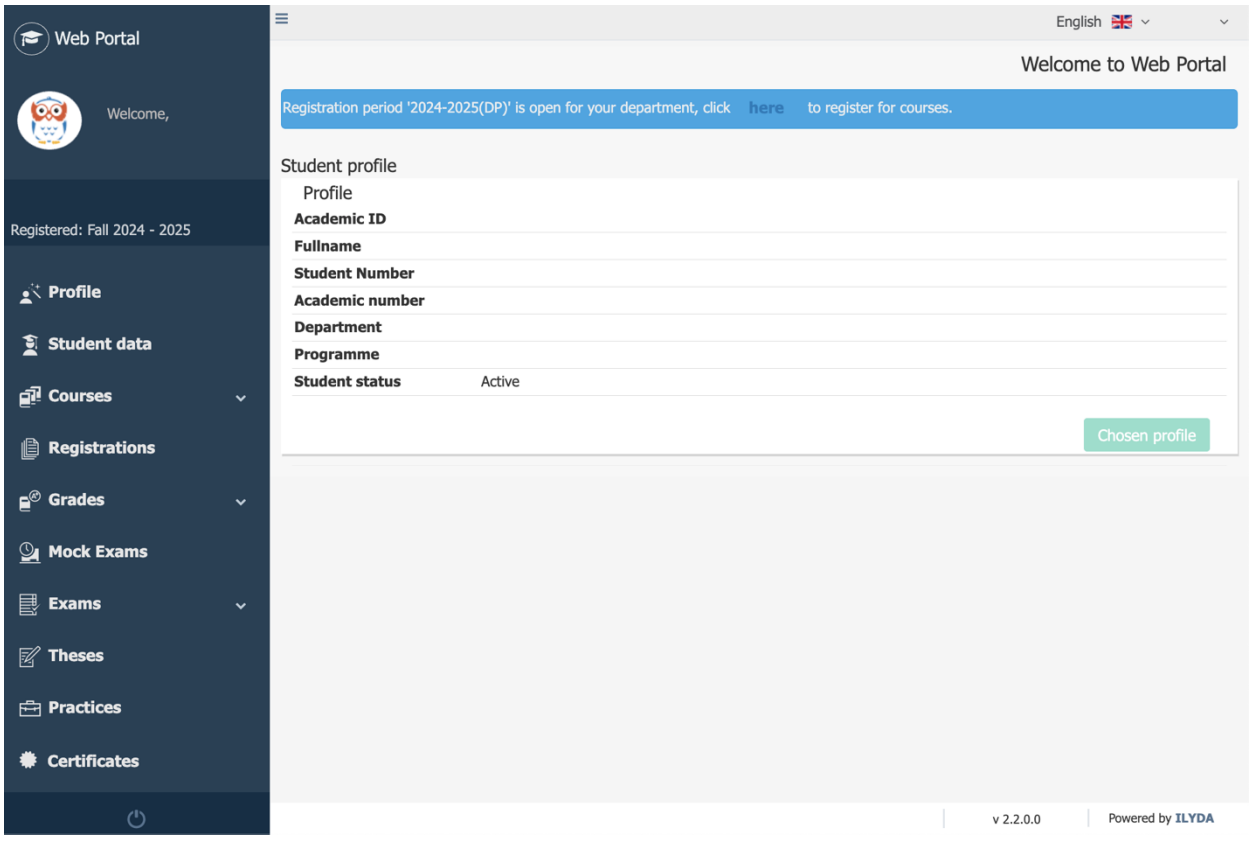


Figure 1: Home page of the Student Information Portal (https://sis-portal.unipi.gr)

3.19.1.6 Synchronous Teaching (Microsoft Teams)

For conducting synchronous teaching (https://www.unipi.gr/en/e-learning/), the University of Piraeus has installed the Microsoft Teams platform, which is centrally supported. The Microsoft Teams platform can support synchronous teaching for an

audience of up to 250 people in real time, through the Microsoft Teams Meetings feature. Additionally, the University has a limited number of shared licenses for the Microsoft Live Events subsystem, which supports the broadcasting of a class to a large audience in near real time.

For the timely preparation and participation of instructors and master's students in distance synchronous teaching, registration in the Delos365 service (https://delos365.grnet.gr/) (see Section 3.19.4.2) with their institutional account (see Section 3.19.3.1) is required.

3.19.1.7 University Laboratories

The M.Sc. utilizes the "Systems Security" laboratory, which is supported by the University and the Department of Digital Systems. It is located in one of the University's buildings at 150, Androutsou Street in Piraeus.

3.19.1.8 M.Sc. Graduates: Electronic Registration in the Club Alumni

To maintain its relationship with its graduates and to explore the contribution of the master's studies to their subsequent careers, the M.Sc. encourages graduates to register electronically in the Club Alumni.

3.19.2 Electronic Services of the Academic Unit

The University operates, among others, asynchronous and synchronous e-learning systems, an academic software distribution service, dinning and housing application services, technical support services, etc. In addition, external services are also available to postgraduate students.

3.19.2.1 University of Piraeus Website

All announcements from the University's services are posted on the University's main website https://www.unipi.gr/en, while additional information is also posted on the Department's and the Master's Program's websites. All information about the electronic services available to the students can be found in the section: Services – E-Services → General Information (https://www.unipi.gr/en/general-information/).

3.19.2.2 Master's Students Dining

Students entitled to free meals can submit, through the Department of Student Care, a free meals application via the University's online platform https://merimna.unipi.gr/?lang=en_US, where applicants can attach the required supporting documents after activating their institutional account. Through the same platform, students meeting the necessary criteria can also apply for accommodation in a

student residence. The relevant instructions are posted on the Department of Student Care website (https://www.unipi.gr/en/student-care/). The Student Restaurant operates in the building at 78 Tsamadou Street. More information is available on the page https://www.unipi.gr/en/dining/

3.19.2.3 University of Piraeus Library

The Library (opening hours: 8:00 – 20:00) of the University of Piraeus offers a wide range of services through its main website: https://www.lib.unipi.gr/iguana/www.main.cls?surl=library

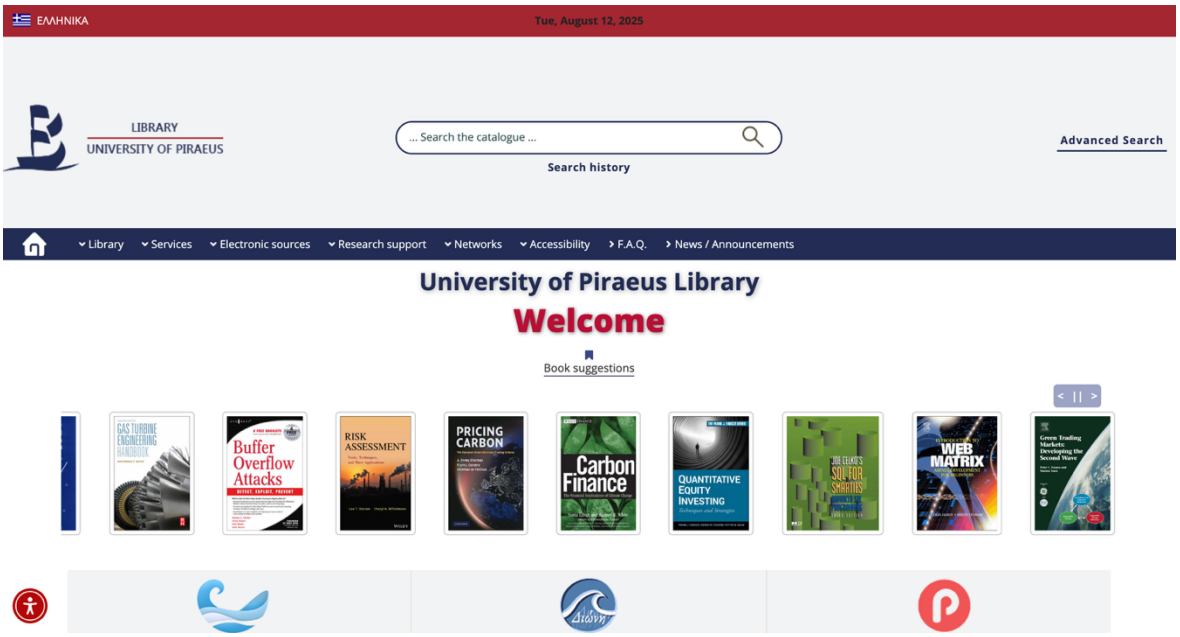


Figure 2: Home page of the University of Piraeus Library (https://www.lib.unipi.gr/iguana/www.main.cls?surl=library)

The library's electronic catalog contains books, dictionaries, journals, special publications for courses, master's students' assignments, as well as books for personal information needs and leisure. The electronic repositories Dioni and Pandora host master's/PhD theses by graduates and articles by the University's faculty and researchers. Master's students can use their academic ID card to borrow books either from the University of Piraeus Library or from partner libraries. They have also access, via HEAL-Link, to countless full-text electronic journals, electronic textbooks (Kallipos), bibliographic databases, and e-books.

All services and information sources offer remote access to University of Piraeus members via VPN (instructions for the VPN service are available at https://www.unipi.gr/en/vpn-connection/).

3.19.2.4 Healthcare

All students who have no other medical and hospital care, are entitled to full medical and hospital care in the National Health System (NHS), with coverage of the relevant costs by the National Health Insurance Fund. More information is available at https://www.unipi.gr/en/health-care/.

3.19.2.5 European Health Insurance Card (EHIC)

The University of Piraeus offers the possibility of issuing the European Health Insurance Card (EHIC) for students who travel to European Union countries and do not have any other medical and hospital care coverage.

3.19.2.6 University Medical Center

Primary health services are provided by the University Medical Center. It operates daily on the ground floor of the main building, office 003. The clinic is fully equipped with medical equipment (cardiograph, defibrillator, and pharmaceutical material for intravenous, intramuscular or oral treatment). The University's population is served daily by a specialist pathologist and a nurse, and occasionally a gynecologist visits the University.

Telephone: +30-210-414-2166 **(in cases of emergency dial the European emergency number 112)**

3.19.2.7 Counseling Center

The University of Piraeus Counseling Center (UCPC) was founded in 1995 and operates as a place of Meeting, Support, Communication and Intervention. The staff of the Counselling Center, recognizing the specificity of the difficulties that students may face, negotiate issues that are important to all and relate to:

- Active learning
- Successful adaptation to new needs and requirements
- Social skills, relationships and family
- Dealing with stressful situations
- Prevention and Health
- Ways of creative expression and entertainment
- Developing skills necessary for success

Interventions and addressing the needs that arise can be done either through individual and group psychological counselling or through the conduct of seminars focusing on the promotion of academic adjustment of the student population.

The Counseling Center is located on the ground floor of the main building of the University of Piraeus, room 018. Contact hours with students: 9:00am-3:00pm. Monday to Friday. Telephone: +30- 210-414-2042

3.19.2.8 Volunteer Team - Kerykes

The volunteer group Kerykes is active at our University. This group participates both in University actions and in actions focused on people, society and the environment.

3.19.2.9 Cultural Groups at the University of Piraeus

The cultural groups of the University of Piraeus offer the members of the University community the opportunity to pursue their interests and cultivate their talents. They promote volunteerism and active student participation and cover a wide range of activities. More specifically, the University of Piraeus has the following cultural groups:

- Theatre Team
- Musical Ensembles
- Modern Dance Group
- Literacy Circle

3.19.2.10 Sports Activities at the University of Piraeus

The University offers a variety of sports activities so that each postgraduate student can participate in physical exercise according to their interests and athletic level. Students can take part in the following sports:

- Basketball
- Volleyball
- Football (Soccer)
- Water Polo
- Tennis
- Chess

3.19.2.11 Digital Notice Board

The University of Piraeus operates a system of digital notice boards placed in central locations throughout the University, through which students are informed about the classes taking place on that day and the lecture rooms where they are held.

3.19.2.12 Teaching and Learning Support Center (TLSC)

The Teaching and Learning Support Center (TLSC) of the University of Piraeus aims to ensure continuous support for teaching and learning processes, as well as to inform and

assist all teaching staff in innovative educational practices. This support is based on the exchange of expertise related to modern educational trends and approaches.

The purpose of the TLSC is to provide immediate, effective, and comprehensive support for the teaching activities of the University's academic staff, as well as to enhance the overall educational experience of master's students, with the goal of creating an optimal learning environment that improves the quality of teaching and learning.

3.19.3 Guidelines for activating the electronic services of the M.Sc.

3.19.3.1 Creation and management of the institutional account

To use the University's electronic services, the first step is to create a University of Piraeus account. Once the entry and verification of the student's information in the Secretariat's Information System is completed by the Secretariat and the registration is finalized, you can visit the service at https://uregister.unipi.gr and activate the account using the mobile phone number or the email address provided during registration.

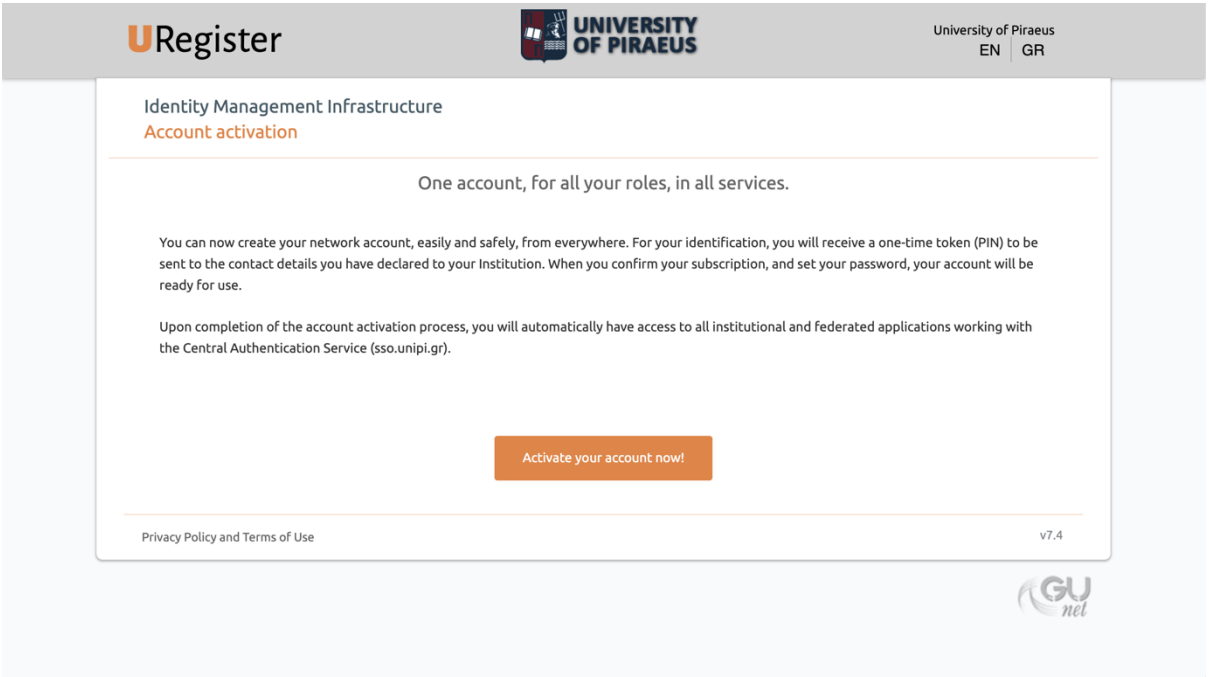


Figure 3: Home page of the uregister service (https://uregister.unipi.gr)

During the *uregister* process, a mobile phone number and email address must be declared for password recovery in case it is lost. The system also verifies certain details (such as e-mail, mobile phone, full name, father's name, and Social Security Number). If there is an error in the information stored in the Ministry of Education's database, a problem will occur during account creation, and the details will need to be corrected

through the Secretariat. More information is available at: https://www.unipi.gr/en/uregister-2/

3.19.3.2 "mypassword" Service

Complementary to the *uregister* service, the *mypassword* service (https://mypassword.unipi.gr) allows you to change your account password using the recovery email or mobile phone number provided when the institutional account was created via *uregister*. It also allows you to update the registered recovery email or mobile phone number stored in the mypassword system. More information is available at: https://www.unipi.gr/en/mypassword-2/.

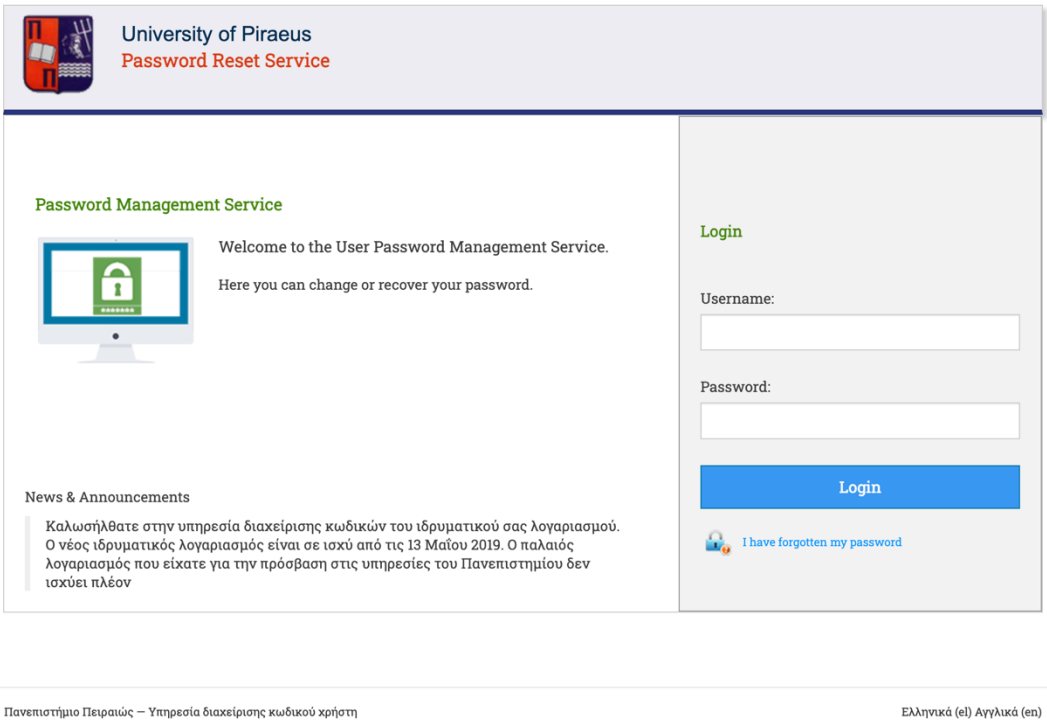


Figure 4: Home page of the mypassword service (https://mypassword.unipi.gr)

3.19.4 Electronic Services of the Ministry of Education, Religious Affairs and Sports

A few hours after the creation of the University account, allowing time for the automated update of intermediate subsystems, it becomes possible to register with the following additional systems:

3.19.4.1 Academic Identity Card Online Service

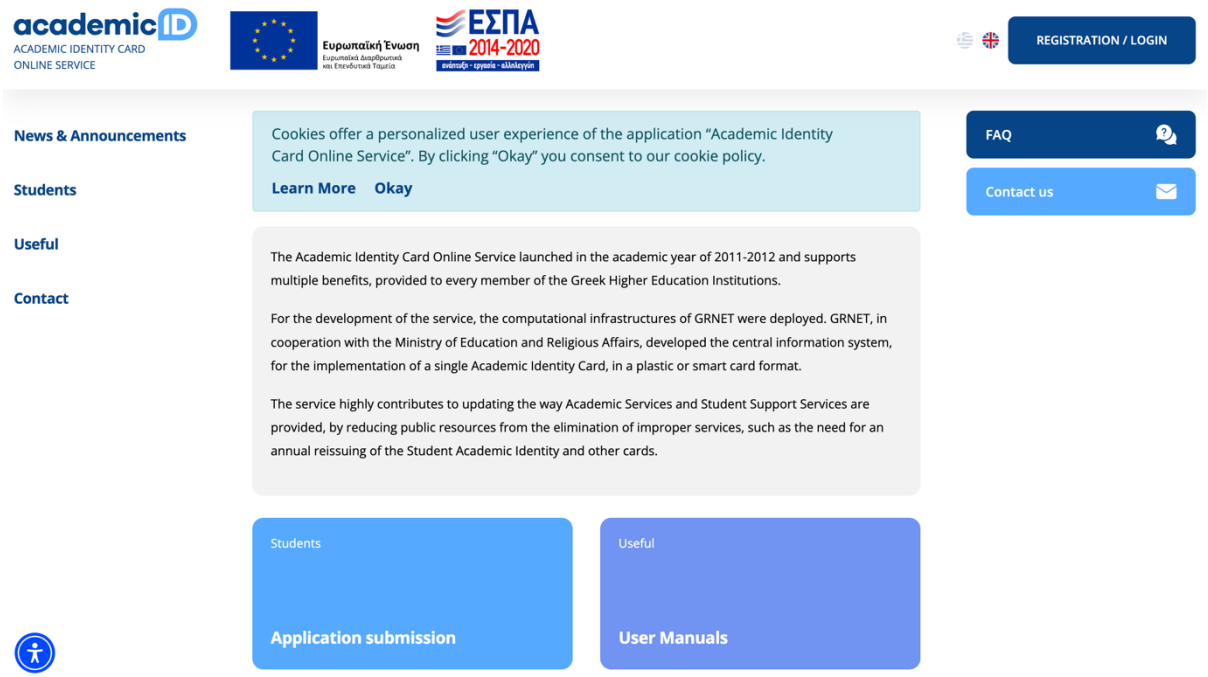


Figure 5: Home page of the Academic Identity Card Online Service (https://academicid.minedu.gov.gr)

After creating the University account, students may register for the Academic Identity Card Online Service (https://academicid.minedu.gov.gr), which also serves as the Student Transportation Card (pass) and is used for identification in the University's academic processes (e.g., examinations).

It should be noted that the Academic Identity Card Online Service is provided directly by the Ministry of Education, Religious Affairs and Sports.

3.19.4.2 DELOS 365 Service

Figure 6: Home page of the DELOS 365 platform (https://delos365.grnet.gr)

By registering on the platform https://delos365.grnet.gr, students gain access to Office365 software and the Microsoft Teams application. Registration simply requires visiting the page and logging in with the University account that has been created. The creation of the Office 365 and Microsoft Teams account takes place directly on Microsoft's online infrastructure and may require up to one day for the full activation of all services. More information is available at: https://helpdesk.unipi.gr/index.php?languageid=1

3.19.5 Supportive services for master's students of the University of Piraeus

In addition to the educational process, the University account may also be used for the following supportive services:

3.19.5.1 Software Distribution Website

Free commercial software for educational use is available through https://helpdesk.unipi.gr/software, where instructions are provided for each available software package. It should be noted that the availability of software depends on the Department of study.

3.19.5.2 Wireless Network Services and Virtual Private Networks (VPN)

For certain services or software use, a connection to the University of Piraeus network is required. This can also be done remotely, from a personal computer, through the Virtual Private Network (VPN) service provided by the University's Network Operation Center, following the instructions available at: https://www.unipi.gr/en/vpn-connection/

Additionally, access is available to the pan-European wireless network Eduroam, which operates in a large number of academic and research institutions in Greece and Europe: https://www.unipi.gr/en/wi-fi-and-eduroam/.

3.19.6 Supportive services for master's students from external providers

In addition to the services of the University of Piraeus, the University account also provides access to services offered by external organizations, which may be needed during studies, such as the following:

- Other services of the National Network of Infrastructures for Research and Technology (GRNET): https://www.unipi.gr/en/national-network-of-infrastructures-for-research-and-technology-hellas-and-research/ and https://grnet.gr/en/education/.

3.20 Rights and Obligations of Postgraduate Students

1. Postgraduate students enjoy all rights and benefits provided to first-cycle students except the free supply of textbooks. The University ensures equal access to its premises for postgraduate students with disabilities or special educational needs and guarantees the accessibility of its physical and digital infrastructure, services, equipment and learning materials.
2. Postgraduate students are expected to participate in and attend activities such as lectures, research-group seminars, laboratory visits, conferences/workshops in fields related to the M.Sc. and other scholarly events of the Programme.
3. Postgraduate students participate in the information-literacy courses conducted by the University Library, which concern: search strategies for information resources and evaluation of results (validity, currency, relevance), compilation of bibliographies and citation standards, information ethics (e.g. avoidance of plagiarism) and self-deposit of Master's Theses in the DIONI Institutional Repository.
4. The Department's Assembly, acting on a recommendation from the Coordinating Committee (C.C.) and after inviting the students concerned to exercise their right to be heard, may decide to dismiss postgraduate students who:
   a) exceed the maximum absence limit

b) have failed a course or courses and have not successfully completed the curriculum
c) exceed the maximum period of enrolment set by the Regulations
d) have committed disciplinary offences as determined by the competent bodies
e) request withdrawal of their own accord
f) fail to pay the prescribed tuition fee when due, wherever and however required.

5. The maximum absence limit per course is 25%. If this limit is exceeded, the student is deemed to have failed the course. If a student's absences exceed 25% in each course of the semester, dismissal is considered; the C.C. examines the case and submits its opinion to the Department's Assembly.
6. For all cohorts of operation of the M.Sc. Programme, within the application process the applicants pay an application fee of two hundred (200) euros. This fee is non-refundable for all candidates, regardless of the evaluation outcome.
7. For the first two (2) cohorts of operation of the M.Sc. Programme, the tuition fees of postgraduate students coming from Greece and the other EU countries are fully covered by the European project **EU-iNSPIRE** (EU iNnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce), financed under the DIGITAL-2023-SKILLS-05 programme (Grant Agreement No. 101190054). For postgraduate students coming from non-EU countries, the tuition fees for these cohorts are five thousand euros (5.000€).
8. From the third (3rd) cohort of operation of the M.Sc. Programme onward, the tuition fees of postgraduate students coming from Greece and the other EU countries are five thousand euros (5.000€), while for postgraduate students coming from non-EU countries the tuition fees are seven thousand euros (7.000€).
9. According to the Postgraduate Studies Regulation, tuition fees are paid in two equal instalments: the first instalment upon the announcement of those admitted to the M.Sc. Programme, to reserve the place (September), and the second instalment at the beginning of the second academic semester.

   Selected postgraduate students who are exempted from tuition fees under the applicable legislation are refunded in full any fees paid up to that time.
10. Enrolled postgraduate students of the M.Sc. Programme who are not citizens of third countries may study free of charge provided they meet the financial or social criteria laid down in the relevant provisions (Article 86 of Law 4957/2022 and Ministerial Decisions 84560/Z1/27-07-2023 and 108990/Z1/08-09-2022). (Clarification: A "third country" is any country outside the European Economic Area (EEA). The EEA countries are the 27 EU Member States plus Iceland, Norway and Liechtenstein). A further prerequisite for a tuition-fee waiver on financial or social grounds (Article 86 of Law 4957/2022) is fulfilment of the excellence criterion in first-cycle studies (Bachelor degree), namely possession of a Bachelor degree with a grade of at least 7.5/10. The total number of postgraduate students studying free of charge under the

above legislation may not exceed 30 % of all enrolled postgraduate students per academic year. Applications for free tuition in each M.Sc. Programme are submitted after completion of enrolment. The Department's Assembly examines whether the waiver criteria are met. The waiver is granted only once, for study in a single M.Sc. Programme organized by a Greek University.

11. The academic calendar and timetable of the M.Sc. Programme are drawn up within the University's academic calendar and approved by the Department's Assembly on the recommendation of the Coordinating Committee (C.C.). Upon enrolment, postgraduate students receive from the Secretariat the annual Academic Calendar of the Programme, which includes the start and end dates of teaching periods, examination periods, holidays, etc.
12. Each candidate, before enrolling in the M.Sc. Programme, must read the M.Sc.'s Operating Regulation and sign a declaration that he or she accepts its rules.

3.21 Awarding of scholarships

According to the Postgraduate Studies Regulation of the Program, the M.Sc. may provide a number of scholarships each academic semester to postgraduate students who pay tuition fees, in accordance with a decision of the Department's Assembly, following a recommendation from the Master Program's Coordinating Committee. The amount of each scholarship cannot exceed the tuition fees of one semester. Scholarships are awarded on the basis of academic criteria during the course of studies in the M.Sc., by decision of the Department's Assembly, following a recommendation from the Coordinating Committee, and are included in the Program's budget. Any obligations of the scholarship recipients are determined in the same decision of the Department's Assembly, again upon recommendation of the Coordinating Committee. If more than one eligible scholarship recipient attains the same grade point, either a lottery will be held among them before the Coordinating Committee, or the scholarship amount will be equally divided among them, following a decision of the Department's Assembly upon recommendation of the Coordinating Committee.

3.22 Student Mobility

Any mobility of postgraduate students of the M.Sc. Programme, whether for study or practical training, is conducted in accordance with the Programme's Mobility Regulation. (Appendix 3: Mobility of students and staff Regulation (ERASMUS+ & ERASMUS+ International)).

3.23 Academic Advisor

For the qualitative enhancement of the master's program's operation, the Academic Advisor has been established and is in effect, placing the master's student at the center

and aims to contribute decisively to their academic and subsequent professional development.

For more information regarding the Academic Advisor, refer to Appendix 4: Regulation on the Functioning of the Academic Advisor.

3.24 Management of Students' Complaints and Appeals

The adoption of the Regulation for managing requests and/or complaints of master's students in the M.Sc. aims at enhancing the quality of the programs' operation. It places at the center the respect for all participants in the educational process, and even more so for the students, who are the primary recipients of this process and to whom accountability is owed. In line with the principles of transparency and accountability, and in order to strengthen the student-centered educational process, this Regulation was developed. It provides a detailed description of the procedure for handling requests/complaints as well as the parties involved.

For more information the Regulation for the Management of Students' Complaints and Appeals of the Postgraduate Program is available in Appendix 5: Regulation for the Management of Students' Complaints and Appeals .

3.25 Evaluation of postgraduate students

3.25.1 Description of the assessment of learning outcomes system

The evaluation of master's students' performance is an integral part of the educational process, as it links teaching with learning and with the assessment of the achievement of learning outcomes. Evaluation takes place throughout the academic semester.

The final evaluation process and grading for individual courses of the M.Sc. are determined by the instructor responsible for the course. In the event that a student fails or does not attend the course examination, the student is given the opportunity to participate in a resit examination. Each postgraduate student may fail up to two (2) courses per academic semester. Failure in three (3) or more courses in the same semester leads to dismissal from the program, following a decision by the Department Assembly, except in special cases of force majeure (such as illness, work overload, etc.), in which case a larger number of failed courses may be permitted. The resit examinations for courses are conducted following the relevant decisions. If a student fails more than twice in the same course, they may, upon submitting a request, be examined by a three-member committee of instructors of the Master's Program. The members of this committee must have the same or a related academic field as the course being examined

and are appointed by the Department Assembly. The instructor responsible for the course examination is excluded from this committee.

3.25.2 Learning Outcomes

Learning outcomes are the statements of what learners know, understand, and can do upon completion of the learning process.

In essence, the learning outcomes of a course include:

- Knowledge: theoretical and/or practical knowledge acquired.
- Skills: understanding and applying the acquired knowledge.
- Competences: demonstrated proficiency in using the acquired knowledge and skills.

that postgraduate students are expected to know, possess, and be able to demonstrate upon the successful completion of the course.

Within the student-centered teaching approach followed, learning outcomes are placed at the core of the learning process. Their achievement is measurable, assessed, and determines the performance of master's students in each educational component. At the beginning of each course, master's students are informed about the expected learning outcomes, the assessment system, and the evaluation criteria for that course by the instructors. They are also encouraged to consult the course syllabus, available on the Department's website, for further details regarding the assessment process and the type of examinations.

3.25.3 Evaluation System

The process of evaluating students per educational activity will be carried out with distance methods such as:

- Quizzes with short answer questions
- Tests (Quizzes) with extended answer questions
- Evaluation of a written paper/report/project (bibliographic topics, independent case studies, problem solving in hypothetical scenarios, etc.)
- Evaluation of laboratory / practical exercises
- Evaluation of participation in the learning process in the context of theoretical or seminar courses and in forums of the Postgraduate Program.
- A combination of two or more of the above methods.

The determination of the way and procedure for the evaluation of students in a course is the sole responsibility of the instructor, to whom the Department's Assembly has assigned the teaching of the course.

The evaluation and grading in each course are done in complete independence from the other courses and is a derivative of the objective assessment of the student's performance in the specific course (assignments, exams, etc.). The evaluation criteria are clearly defined; they are communicated at the beginning of the academic semester by the instructor in charge/coordinator of the course and are also indicated in the description form (outline) of each course that is posted on the website of the M.Sc. Postgraduate Program.

The final grade of each course results from the student's total performance in specific areas (e.g. assignments, examinations) according to the instructions provided by the instructor at the beginning of the semester. The minimum acceptable course grade is five (5.00), with a maximum of ten (10.00), with the possibility of grading in the form X.5. Each course included in the curriculum, as well as the Master Thesis, is graded independently.

Especially for the written papers prepared in the context of each course, these are evaluated on the basis of criteria of the perfect selection of bibliographic sources, the scientific correctness of the analysis of existing knowledge, the deepening of the field, the range of coverage of the subject, the accuracy in the description, the coherent structure and clear depiction of the arguments of the final text, the overall scientific maturity of the work, the conformity of the appearance and contents of the work with the relevant instructions. The evaluation criteria are further specified and analyzed, where necessary, in the presentation of the instructors during the first lecture of the course.

The feedback on the degree of satisfaction of postgraduate students with the criteria and the method of evaluation is obtained from the students' evaluation questionnaires.

The Master's Theses are assessed based on criteria such as the appropriate selection of bibliographic sources, the scientific accuracy of the analysis of existing knowledge, depth of field research, breadth of subject coverage, descriptive accuracy, coherent structure and clear articulation of arguments, research contribution and generation of new knowledge in the scientific field, the overall scientific maturity of the work, compliance with the formatting and content guidelines, as well as completeness and maturity during the oral presentation, consistency with the allocated time, and the scientifically sound responses of the postgraduate student to the questions posed by the Examination Committee.

Grading criteria include:

Grade [9-10]

- Demonstrates excellent understanding of all major issues
- Relevant literature has been thoroughly researched and critically evaluated
- Advanced ability to apply theory in approaching practical problems (where appropriate)
- Highly informative interpretation of findings with critical awareness of both strengths and limitations
- Accurate use of tables and figures
- Well-selected and up-to-date references used at appropriate points
- Complete and well-structured bibliography
- Exceptionally well-organized and fully developed thesis within the word limit.

Grade [8-9)

- Demonstrates comprehensive understanding of key issues
- Relevant literature has been satisfactorily researched and evaluated
- Ability to apply theory in a refined manner to practical problems
- Major issues arising from the topic are identified and addressed wholly or partially
- No significant factual or interpretative errors
- Sound and effective use of tables and figures
- Well-selected and updated references used at appropriate points
- Well-organized and logically structured thesis within the word limit.

Grade [7-8)

- Demonstrates satisfactory understanding of key issues with some gaps or deficiencies
- Literature has been researched at an acceptable but not beyond that
- Satisfactory ability to apply theory to practical problems (where appropriate)
- Some major issues arising from the topic are identified and addressed
- Few factual or interpretative errors indicating some misinterpretation of the literature
- Mostly appropriate tables and figures
- Adequate references with some omissions and acceptable use of sources
- Logical structure with occasional inconsistencies within the word limit.

Grades [5-7)

- Demonstrates less than satisfactory understanding of key issues
- Literature has been partially researched, leaving significant gaps
- Limited ability to relate research to practical problems (where appropriate)
- Several major issues arising from the topic are not sufficiently addressed
- Some serious factual or interpretative errors indicating misunderstanding of core material
- Inappropriate or incomplete use of tables and figures
- Inappropriate or incomplete references

- Presentation, pagination, title, margins, and paragraphs not in accordance with relevant guidelines.

Grades [1-4] (unsuccessful)
- Demonstrates inability to understand key issues
- Literature has been inadequately researched, revealing knowledge gaps
- Very limited ability to relate research to practical problems (where appropriate)
- Few to none of the major issues arising from the topic are identified or presented
- Serious factual and interpretative errors
- Inappropriate or incomplete use of tables and figures
- Inappropriate or incomplete references
- Careless presentation, insufficient attention to pagination, title, margins, and paragraphs.

Grade 0
- No thesis submitted

3.25.4 Adaptation of the evaluation system for master's students with serious conditions and learning difficulties

In addition to the provisions outlined above, students who submit to the M.Sc. Secretariatdiagnostic certificates proving health issues, such as vision, hearing, mobility problems, dyslexia, or other disorders, which make it difficult for them to participate in written or oral examinations, are granted special provisions to facilitate and adapt the examination process, in accordance with the applicable legal framework and with the support of the instructors. Indicatively::

- Provision of additional examination time, depending on the case
- Oral examination for students unable or struggling to write, those requiring support during the examination, or those who have difficulty participating in oral group examinations
- Adjustment of the visual presentation of questions, e.g., proportional enlargement of text size in cases of vision impairment
- Reading aloud of the examination questions where necessary
- Use of converters (assistive technology) when required
- Additional accommodations for students with mobility impairments, depending on the case and within the framework of the available equipment and infrastructure of the University of Piraeus (see Section 3.30.2).

3.26 Procedures and criteria for the selection of teaching staff

By decision of the Department Assembly, teaching duties may be assigned to faculty members (DEP) of the Department of Digital Systems, as well as to faculty members of

other departments of the University or departments of other universities in Greece or abroad (primarily from the collaborating academic institutions – see Section 3). Teaching may also be assigned to other categories of instructors in accordance with the provisions of Law 4957/2022 (A141), as in force, and the Regulation for the 2nd and 3rd Cycle Study Programs of the University. The specific requirements and the procedure for inviting instructors from Greece or abroad, as well as the specific terms of employment and any other matters related to instructors belonging to the categories described in cases (e), (st), and (z) of paragraph 1 of Article 83 of Law 4957/2022, shall be determined by a decision of the Department Assembly, within the framework of the applicable legislation.

By decision of the Department's Assembly, auxiliary teaching duties may also be assigned to doctoral candidates of the Department or the School, under the supervision of an instructor of the M.Sc..

The assignment of teaching duties in the M.Sc. is made by decision of the Department's Assembly, following a substantiated recommendation from the Program's Coordinating Committee (C.C.), or otherwise by the M.Sc. Director. The recommendation submitted by the Coordinating Committee takes into account as criteria the relevance of the instructor's specialty, experience, teaching and research work to the course subject being assigned, as well as to the M.Sc. in general. If there are available results of evaluations of the instructors' teaching ability, these are also considered in the recommendation.

Each course is taught by one or more instructors. For each course, the Department's Assembly appoints one instructor as the course coordinator. The selection of the coordinator takes into account the experience and academic work of the instructor, as well as their availability to carry out the coordinator's responsibilities.

3.27 Graduation Ceremony/ Oath-Taking

A postgraduate student who has successfully completed the M.Sc. studies formally declares /takes an oath at a ceremony held in the presence of the Rector (or a Vice-Rector acting on the Rector's behalf), the Dean of the School, the Head of the Department, and the Director of the M.Sc. Programme. Although the oath is not a constitutive element of completing the programme, it is a necessary condition for the award of the Master's diploma.

For reasons of force majeure, a graduate may apply to the Department's Secretariat to receive the M.Sc. diploma without attending the declaration/oath-taking ceremony or may request to participate in a subsequent ceremony. Before the ceremony -or exemption from it- a certificate confirming successful completion of studies may be issued to the graduate.

The wording of the declaration/oath for graduates receiving an M.Sc. is determined by decision of the Senate. Graduates who do not wish to take a religious oath may instead make a simple affirmation on their honour and conscience.

3.28 Infrastructure and Funding of the M.Sc. Program

To ensure the smooth operation of the M.Sc. Programme, teaching and seminar rooms, auditoria equipped with audiovisual facilities, and University laboratories are made available.

Core funding for the first two (2) cohorts of the Programme is provided by the European project **EU-iNSPIRE** (EU iNnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and Reskilling the EU workforce). The project commenced in January 2025, runs for four (4) years, and is financed under the DIGITAL-2023-SKILLS-05 call (Grant Agreement No. 101190054). Specifically, the organizational and operating costs of the Programme (including the tuition fees of postgraduate students from Greece and other EU member states) are covered for these first two cohorts by the project's funding, by application fees, and by the tuition fees of postgraduate students from non-EU countries.

From the third (3rd) cohort onward, funding will be drawn from donations, endowments, sponsorships, research projects, programmes of the EU or other international organizations, application and tuition fees of all postgraduate students from Greece, other EU countries, and third countries, as well as any other sources permitted by the applicable legislation.

3.29 Evaluation of the M.Sc. Program

At the end of each semester, every course and every instructor is evaluated by the postgraduate students. The accreditation of the M.Sc. Program is carried out by the Hellenic Authority for Higher Education (HAHE), in accordance with the applicable legislation.

Within this framework, the evaluation assesses the overall performance of the M.Sc. Program, the degree to which the objectives set at its establishment have been achieved, its sustainability, the employability of its graduates, the Program's contribution to research, its internal evaluation by postgraduate students, the advisability of extending its operation, and other elements relating to the quality of the work produced and its contribution to the national strategy for higher education.

For the continuation of its operation, the M.Sc. Program must undergo periodic accreditation as part of the regular evaluation/accreditation process of the Department of Digital Systems. The M.Sc. Program may also be accredited by other bodies, should it so choose.

Through the Student Information System Portal (https://sis-portal.unipi.gr/), students confidentially complete evaluation questionnaires for each course, each instructor, and the M.Sc. Program's facilities.

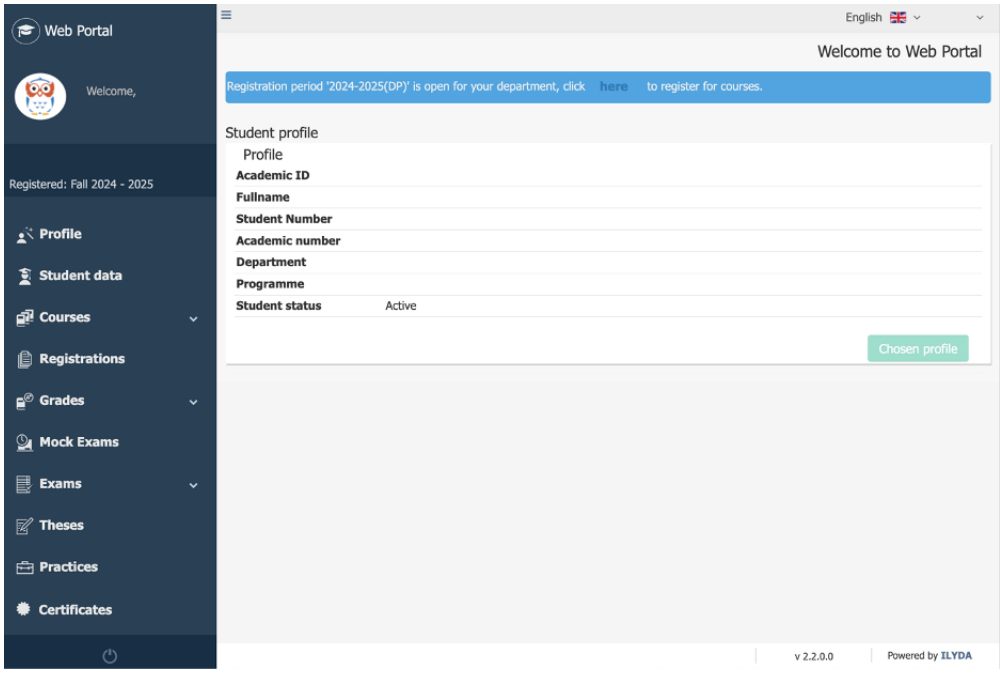


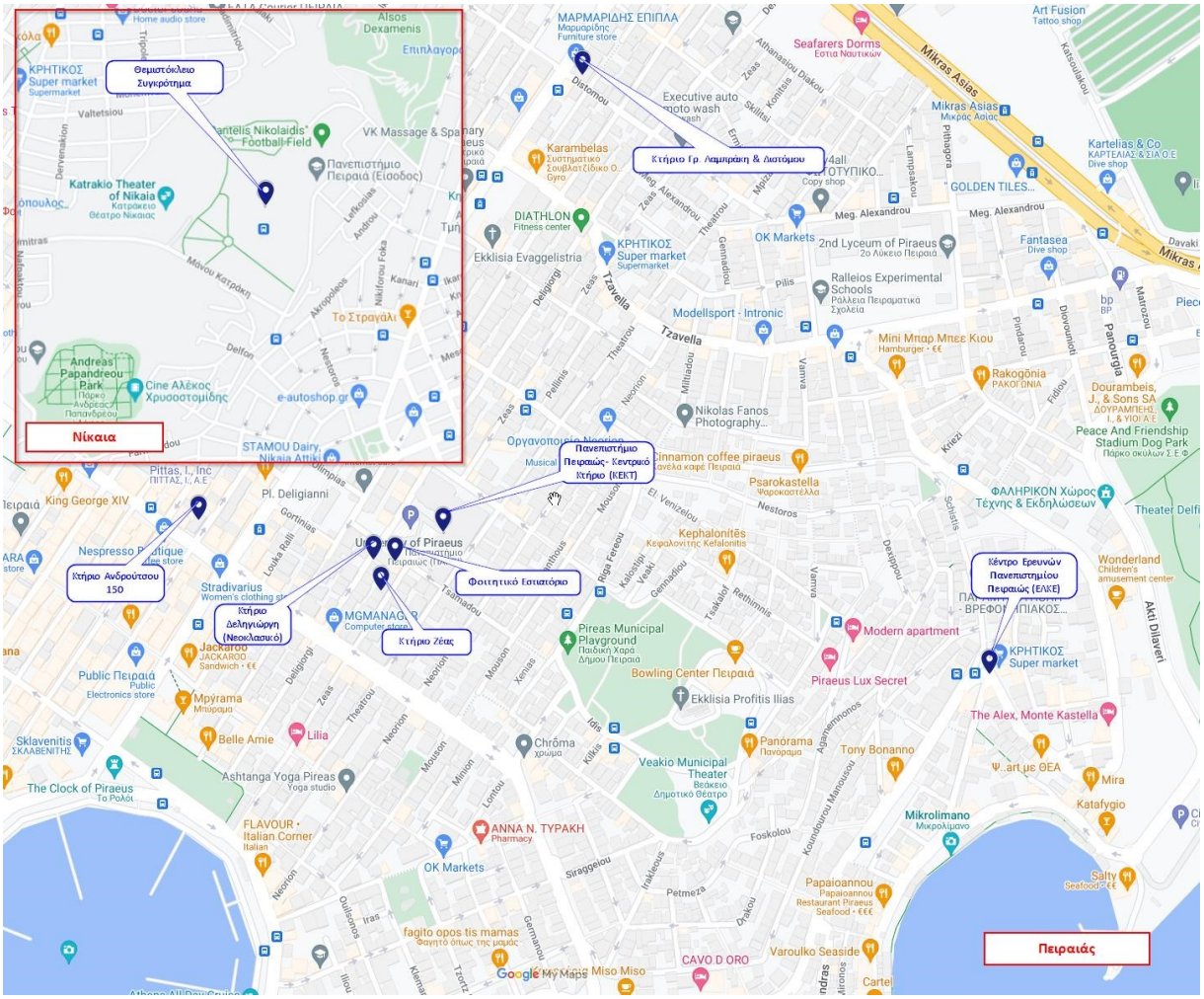
Figure 7: Homepage of the Online Student Administration Service (https://sis-portal.unipi.gr)

3.30 Access to the Premises of the University of Piraeus

3.30.1 Access to the University Premises by Public Transportation

The link below provides a map of the University of Piraeus buildings, while the subsequent table specifies the available means of transportation for reaching each building.

University of Piraeus Buildings- Google Maps (click on the link)



UNIVERSITY OF PIRAEUS BUILDINGS	ADDRESS
University of Piraeus (Central Building) (ΚΕΚΤ)	80 Karaoli & Dimitriou St., Piraeus 185 34
University of Piraeus- Neoclassical Building (ΝΕΟΚΛ/ΔΕΛ107)	107 Deligiorgi St., Piraeus 185 34
University of Piraeus- Gr. Lambraki Building (ΓΛ21)	43 Distomou St., Piraeus 185 33
University of Piraeus- Androutsou Building (ΑΝΔ150)	150 Odyssea Androutsou St., Piraeus 185 32
University of Piraeus- Zeas Building	82 Zeas St., Piraeus 185 34
University of Piraeus Student Restaurant	78 Tsamadou St., Piraeus 185 34
University of Piraeus- Themistokleio Complex /Weightlifting Building (NIKAIA Α, Γ, Δ)	17 Kyras Tis Ro St., Nikaia 184 51
University of Piraeus Research Center	91 Alexandrou Papandreou Ave., Piraeus 185 33

3.30.2 Accessibility Infrastructure for Persons with Disabilities

The University of Piraeus has implemented a range of measures to ensure accessibility for individuals with reduced mobility and sensory disabilities. These include:

- Safe operation of elevators
- Adaptation of restroom (W.C.) layouts
- Installation of special lifts/platforms for persons with disabilities
- Construction of ramps
- Placement of railings of appropriate design and height (balconies, entrances, etc.)
- Installation of handrails
- Designated parking spaces with floor markings located near elevators

Each building used by the M.Sc. is accessible to persons with disabilities via at least two entrances:

1. The main entrance
2. The underground parking areas

Within the interior spaces of the buildings, fire compartments have been provided in accordance with approved fire safety studies. These studies include designated movement areas (elevators) that may also serve as emergency escape routes in the event of necessity.

3.31 Contact Information

3.31.1 Department's Academic Secretariat

Address: 80–82 Zeas Street (2nd floor), P.C. 18532, Piraeus
Secretariat Group E-mail: gramds@unipi.gr

Full name: Paraskevi Antoniou (Head)
Tel.: +30-210-414-2235
E-mail: panton@unipi.gr

Full name: Sofia Skountzou
Tel.: +30-210-414-2373
E-mail: sskountz@unipi.gr

Full name: Ioannis Frentzas
Tel.: +30-210-414-2426
E-mail: fretzas@unipi.gr

Full name: Panagiotis Theodoropoulos
Tel.: +30-210-414-2369
E-mail: ptheodor@unipi.gr

3.31.2 M.Sc. Program's Secretariat

Address: 150 Odyssea Androutsou Street (1st floor, Office 103), P.C. 18532, Piraeus
(Office hours: 10:00–16:00))
Telephone: +30-210-414-2757
Website: https://cybersecgov-res.ds.unipi.gr/en/home/

E-mail: cybersecgov_res@unipi.gr

3.31.3 M.Sc. Program's Social Media

The M.Sc. Program's social media accounts are as follows:

Facebook: https://www.facebook.com/cybersecgovres/
Linkedin: https://www.linkedin.com/company/cybersecgov-res
Instagram: https://www.instagram.com/cybersecgov_res.msc/

4 APPENDICES

4.1 Appendix 1: Application for Admission to the Master Program

Photograph *(to be affixed here)*

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

Master of Science

in

"Advanced Cybersecurity Technologies and Governance by Research"

APPLICATION FOR ADMISSION TO THE MASTER PROGRAM

Personal Information			
Surname		**First Name**	
Date of Birth		**Email**	
ID Card or Passport Number		**Mobile Phone**	
Home Address			
Mailing Address *(if different from home address)*			
Landline Phone			

Academic Studies

Undergraduate Studies

University	Department	Graduation Date	Degree Grade

Postgraduate Studies

University	Department	Graduation Date	Diploma Grade

- Final-year students who are expected to complete their studies before the start of the new academic year may also participate in the application and evaluation process. Acceptance of such students is conditional upon submitting a certificate of completion of studies from the Secretariat of their Department during the enrollment period of this M.Sc.
- Candidates holding a first-cycle degree from foreign institutions must submit their degree for verification to ensure that the institution is listed in the National Registry of Recognized Foreign Institutions, as well as in the National Registry of Degree Types of Recognized Foreign Institutions. In all cases, foreign degrees must be submitted and will be accepted in accordance with the applicable regulations.

Foreign Languages (* see note at the end)

Language	Proficiency Level	Certificate/Diploma

Undergraduate Theses (for graduates / final-year undergraduate students), Diploma Theses (for graduates / final-year engineering students), Master's Theses (for holders of a Master degree)

Type of Thesis	Thesis Title	Supervising Professor	Grade

Awards, Distinctions, Scholarships

Professional Experience

Position	Organization	Period of Employment	
		from: *Month/Year*	*to:* *Month/Year*

Research Activity

(Any research papers or research projects in which you have participated)

Recommendation Letters

(Details of two individuals from whom you have obtained a recommendation letter)

	Name / Surname	Title	Institution/Organization	Telephone	e-mail
1					
2					

Other Postgraduate Programs to which you have applied or intend to apply

Institution	Title

Source of Information Regarding the Master's Programs of the Department of Digital Systems

☐	Website	☐	Social media	☐	Friend/Acquaintance

☐	Graduate of the Master's Program	☐	Department Information Day	☐	Other

Additional Information

(please include any details you believe may strengthen your application)

Attached Supporting Documents

	MANDATORY
☐	Detailed Curriculum Vitae
☐	Simple copies of academic degrees or other documents (e.g., certificate of completion, academic transcript) proving graduation (for final-year students, proof that they are pending graduation)
☐	Simple academic transcript (one for each degree obtained)
☐	Simple proof of good knowledge of the English language
☐	Two (2) Recommendation Letters (may be sent electronically, directly by the referees, to the following email address: cybersecgov_res@unipi.gr)
☐	Simple copies of any scientific papers and publications
☐	Simple photocopy of passport or national identification document
☐	One (1) photograph
	OPTIONAL
☐	
☐	

(*) Proficiency in the English language may be demonstrated by:

• FIRST CERTIFICATE IN ENGLISH of the University of Cambridge or Cambridge Assessment English, overall score 160–179.

• CERTIFICATE IN ADVANCED ENGLISH of Cambridge Assessment English, overall score 160–179.

• BULATS English Language Test, score 60–74, of the University of Cambridge or Cambridge Assessment English (for certificates issued up to 19/11/2019).

• INTERNATIONAL ENGLISH LANGUAGE TESTING SYSTEM (IELTS) from the University of Cambridge Local Examinations Syndicate (UCLES) or Cambridge Assessment English – The British Council – IDP Education Australia IELTS Australia, score 5.5 to 6.5.

•BUSINESS ENGLISH CERTIFICATE – VANTAGE (BEC VANTAGE) from the University of Cambridge Local Examinations Syndicate (UCLES) or Cambridge Assessment English, overall score 160–179.

• BUSINESS ENGLISH CERTIFICATE – PRELIMINARY of Cambridge Assessment English, overall score 160–170.

• PRELIMINARY ENGLISH TEST of Cambridge Assessment English, overall score 160–170.

• CERTIFICATE OF COMPETENCY IN ENGLISH (ECCE) from the University of Michigan (English Language Institute or Cambridge Michigan Language Assessments – CaMLA or Michigan Language Assessment).

• LONDON TESTS OF ENGLISH LEVEL 3 – Upper Intermediate Communication – of Edexcel, or PEARSON TEST OF ENGLISH GENERAL LEVEL 3 – Upper Intermediate Communication – of Edexcel, or Edexcel Level I Certificate in ESOL International (CEF B2), or Pearson Edexcel Level I Certificate in ESOL International (CEF B2) (English International Certificate).

• CERTIFICATE IN INTEGRATED SKILLS IN ENGLISH ISE II of Trinity College London.

• CITY & GUILDS Level 1 Certificate in ESOL International (Reading, Writing, Listening) – Communicator – and CITY & GUILDS Level 1 Certificate in ESOL International (Spoken) – Communicator – (both submitted together to prove good knowledge), or CITY & GUILDS Certificate in International ESOL – Communicator – and CITY & GUILDS Certificate in International Spoken ESOL – Communicator – (both submitted together to prove good knowledge).

•Assessment Board for Language Examinations: Level B2 (ABLE B2) of the Hellenic American University (Nashua, New Hampshire, USA)

•TEST OF ENGLISH FOR INTERNATIONAL COMMUNICATION (TOEIC) of the Educational Testing Service/Chauncey, USA, score 505–780.

• EDI Level 1 Certificate in ESOL International JETSET Level 5 (CEF B2) or Pearson EDI Level 1 Certificate in ESOL International (CEF B2) or Pearson LCCI Level 1 Certificate in ESOL International (CEFR B2).

•PEARSON LCCI EFB Level 3 (modules: Reading, Writing, Listening, Speaking, with at least "Pass" in one module).

• PEARSON LCCI EFB Level 2 (modules: Reading, Writing, Listening, Speaking, with grade "Distinction" or "Credit").

• OCNW Certificate in ESOL International at Level 1 (CEFR B2) (up to 31/8/2009).

• Ascentis Level 1 Certificate in ESOL International (CEF B2)

• ESB Level 1 Certificate in ESOL International All Modes (Council of Europe Level B2).

• Michigan State University – Certificate of English Language Competency (MSU – CELC) : CEF B2.

• Test of Interactive English, B2 + Level (ACELS)

• Test of Interactive English, B2 Level (ACELS) ή Test of Interactive English, B2 Level (Gatehouse Awards).

• NOCN Level 1 Certificate in ESOL International (B2).

•AIM Awards Level 1 Certificate in ESOL International (B2) (Modules: Listening, Reading, Writing, Speaking) ή AIM Qualifications Level 1 Certificate in ESOL International (B2) (Anglia Advanced) (Modules: Listening, Reading, Writing, Speaking).

• MICHIGAN ENGLISH LANGUAGE ASSESSMENT BATTERY (MELAB) score 80–90 from Cambridge Michigan Language Assessments or Michigan Language Assessment.

• MET – MICHIGAN ENGLISH TEST (Modules: Listening, Reading, Speaking), score 157–189 from Michigan Language Assessment or Cambridge Michigan Language Assessments (CaMLA), or MET – MICHIGAN ENGLISH TEST (modules: Listening, Reading, or Listening, Reading, Speaking, Writing) score 53–63 from Michigan Language Assessment.

• LRN Level 1 Certificate in ESOL International (CEF B2)

• GA Level 1 Certificate in ESOL International –(CEFR: B2) ή GA Level 1 Certificate in ESOL International (Classic B2)

• LanguageCert Level 1 Certificate in ESOL International (Listening, Reading, Writing) (Communicator B2) and LanguageCert Level 1 Certificate in ESOL International (Speaking) (Communicator B2) (both submitted together to prove good knowledge).

• Open College Network West Midlands Level 1 Certificate in ESOL International (CEFR B2)

• NYLC –NEW YORK LANGUAGE CENTER CERTIFICATE Level B2

• LanguageCert Test of English (LTE) - LanguageCert Level 1 Certificate in ESOL International (Listening, Reading) (LanguageCert Test of English B2)

• OCNLR Level 1 Certificate in ESOL International (CEFR B2)

• VTCT (ITEC) Level 1 Certificate in ESOL International (B2)

or the State Certificate of Language Proficiency (SCLP) at Level B2, in accordance with Law 2740/1999, as amended by paragraph 19, Article 13 of Law 3149/2003.

I hereby declare that:

1. The information provided in this application and the attached supporting documents is complete and accurate.
2. I will submit copies of the required documents upon registration in the M.Sc. Program.

3. If I do not submit proof of completion of my undergraduate studies and proof of good knowledge of the English language by September 30 of the current year, my enrollment in the M.Sc. Program will not take place.
4. The amount of the first installment of tuition fees paid upon my acceptance will not be refunded for any reason (except for postgraduate students who do not graduate by the end of September).
5. From the third cohort of operation onwards, if I am among the students exempted from tuition fees under the applicable legislation, any tuition fees already paid will be refunded in full.
6. I have read, understood, and agree with the content of the "Personal Data Protection Policy" for applicants to the M.Sc. Program of the Department of Digital Systems of the University of Piraeus, attached at the end of this application, as well as with the purposes of processing my personal data described therein, and with the current Regulations of the M.Sc. Program.

Date

Applicant's Name

Signature

4.2 Appendix 2: Recommendation Letter Template

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

Master of Science

in

"Advanced Cybersecurity Technologies and Governance by Research"

RECOMMENDATION LETTER

INSTRUCTIONS

- Please fill in the required information about the candidate in the fields below.
- If you prefer, you may use your own letterhead to write the recommendation letter, which we kindly ask you to attach to this page. In that case, please take into account the information requested in this form.
- If the letter is not sent to us directly by email, it should be delivered sealed in an envelope.

Thank you for your assistance!

Candidate Information			
Full Name			
Referee Information			
Referee's Full Name			
Title		**Institution/Organization / Company**	
Address			
Telephone		**E-mail**	

How long and in what capacity have you known the candidate?

If the candidate attended courses you taught, which courses did they take, what grade did they receive in each course, and what was their relative ranking in the class?

Please comment on the candidate's skills and abilities in oral and written communication, collaboration with others, and timely achievement of goals.

Please explain the reasons why you recommend the candidate for this specific postgraduate program.

DO YOU RECOMMEND THIS CANDIDATE FOR ADMISSION TO THE SPECIFIC POSTGRADUATE PROGRAM?	
☐	Strongly recommend
☐	Recommend with reservations
☐	Do not recommend
☐	No opinion / Not sure

Date

Referee's Signature

4.3 Appendix 3: Mobility of students and staff Regulation (ERASMUS+ & ERASMUS+ International)

The Mobility of students and staff Regulation (ERASMUS+ & ERASMUS+ International Program) is detailed in the document "*D5.2b. Mobility of students and staff Regulation (ERASMUS+ & ERASMUS+ International)*". It is posted on the website of the Postgraduate Program and is updated whenever changes occur.

4.4 Appendix 4: Regulation on the Functioning of the Academic Advisor

The Regulation on the Functioning of the Academic Advisor is detailed in the document «D4.*4. Regulation on the Functioning of the Academic Advisor of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»*". It is posted on the website of the Postgraduate Program and is updated whenever changes occur.

4.5 Appendix 5: Regulation for the Management of Students' Complaints and Appeals

The Regulation for the Management of Students' Complaints and Appeals of the Postgraduate program is detailed in document "*D4.3. Regulation for the Management of Students' Complaints and Appeals of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»*". It is posted on the website of the Postgraduate Program and is updated whenever changes occur.

4.6 Appendix 6: Regulations for the Preparation of Assignments

The Regulation for the Preparation of the Master's Thesis are detailed in the document "*D5.2c. Assignment preparation Regulation of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»*". It is posted on the website of the Postgraduate Program and are updated whenever changes occur.

4.7 Appendix 7: Master Thesis Preparation Regulation

The Master Thesis Preparation Regulation of the M.Sc. «*Advanced Cybersecurity Technologies and Governance by Research*» is detailed in the document *"D5.2d. Master Thesis Preparation Regulation of the M.Sc. «Advanced Cybersecurity Technologies and Governance by Research»"*. It is posted on the website of the Postgraduate Program and is updated whenever changes occur.