ΔΙΠΑΕ
CYQAA
ΦΟΡΕΑΣ ΔΙΑΣΦΑΛΙΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΗΣ ΑΝΩΤΕΡΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
CYPRUS AGENCY OF QUALITY ASSURANCE AND ACCREDITATION IN HIGHER EDUCATION
eqar enqa.

Doc. 300.1.2

Date: 7.8.2023

Higher Education Institution's Response

- **Higher Education Institution:**
  European University Cyprus

- **Town:** Nicosia

- **Programme of study**
  Name (Duration, ECTS, Cycle)

  In Greek:
  "Ασφάλεια Κυβερνοχώρου (18 Μήνες/90 ECTS, Μεταπτυχιακό)"

  In English:
  "Cybersecurity (18 Months/90 ECTS, Master of Science)"

- **Language(s) of instruction:** English

- **Programme's status:** Currently Operating

- **Concentrations (if any):**

  In Greek: Concentrations
  In English: Concentrations

ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
REPUBLIC OF CYPRUS

The present document has been prepared within the framework of the authority and competencies of the Cyprus Agency of Quality Assurance and Accreditation in Higher Education, according to the provisions of the "Quality Assurance and Accreditation of Higher Education and the Establishment and Operation of an Agency on Related Matters Laws" of 2015 to 2021 [L.136(I)/2015 – L.132(I)/2021].

A. Guidelines on content and structure of the report

- *The Higher Education Institution (HEI) based on the External Evaluation Committee's (EEC's) evaluation report (Doc.300.1.1 or 300.1.1/1 or 300.1.1/2 or 300.1.1/3 or 300.1.1/4) must justify whether actions have been taken in improving the quality of the programme of study in each assessment area. The answers' documentation should be brief and accurate and supported by the relevant documentation. Referral to annexes should be made only when necessary.*

- *In particular, under each assessment area and by using the 2nd column of each table, the HEI must respond on the following:*

    - *the areas of improvement and recommendations of the EEC*
    - *the conclusions and final remarks noted by the EEC*

- *The institution should respond to the EEC comments, in the designated area next each comment. The comments of the EEC should be copied from the EEC report **without any interference** in the content.*

- *In case of annexes, those should be attached and sent on separate document(s). Each document should be in *.pdf format and named as annex1, annex2, etc.*

1. Study programme and study programme's design and development

(ESG 1.1, 1.2, 1.7, 1.8, 1.9)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
1.1 In terms of the *programme content*, the field of cybersecurity can be schematically summarised as three broad topics: ● *Systems construction* – How do you construct systems that are as secure as possible? ● *Audit, Governance* – Given a system, how do you – continuously – ensure that they remain secure? ● *Incident Planning, Response, Forensics* – Given a system, once it is compromised, what is the proper posture? Considering that the mandatory courses of this programme are "Introduction to Cybersecurity", "Communications and Network Security", "Cryptography", "Policy, Governance, Law, and Compliance", "Cybersecurity Architectures and Operations" and "Ethical Hacking and Penetration Testing", the programme partly covers the first of these topics – *"Systems Construction"* – though, given the evolution of the digital society over the past 5 years since the inception of the programme, inclusion of topics such as "DevSecOps", "Embedded Systems Security", and "Cloud Security" as part of the core curriculum could constitute a	We endorse the EEC recommendation. Indeed, the field of Cybersecurity is rapidly changing and requires syllabus adaptation. We have therefore, enriched our current core courses to include the topics suggested by the EEC as follows: • "DevSecOps" in the course *CYB620 Cybersecurity Architecture and Operations* • "Embedded Systems Security" in the course *CYB620 Cybersecurity Architecture and Operations*, and • "Cloud Security" in the course *CYB605 Communications and Network Security.* Moreover, we have updated the course *CYB655 Incident Response and Forensic Analysis* course to add the latest trends in incident response and forensics analysis and enrich its content due to the development of a separate dedicated course on Cyber Threat Intelligence. We have highlighted for the convenience of the EEC and CY.Q.A.A. with yellow highlights the additions and adjustments made on the respective syllabi (please see updated syllabi of all courses in Appendix I).	Choose level of compliance:

meaningful update which reflects and responds to discipline and professional developments and needs.		
1.2 In view of the increasing prevalence of cyberattacks, and the necessity of dealing with the fall-outs from these competently (something which the interviews with recent-graduates from the programme amply illustrated are part and parcel of the job of even recent graduates) it is surprising to see the topic of *“Incident Planning, Response, Forensics”* covered only through the electives “Risk Analysis and Management” and “Incident Response and Forensic Analysis”. Including these topics as part of the core curriculum could constitute a meaningful update.	Incident response and forensics analysis is one of the most selected topics in the Master in Cybersecurity. Thus, and taking EEC’s comments into consideration, we have enriched our *CYB600 Introduction to Cybersecurity* syllabus with Incident Planning, response and forensics topics so that all students get acquainted with these notions very early in their programme of study. Students will thus gain a high-level understanding of incident management processes, the development of an IRP, incident detection and containment techniques, incident recovery, and the basics of digital forensics. In this way, the course, as expected by the EEC, will provide a solid foundation for further exploration and specialization in these areas within the field of cybersecurity, as provided in the elective course *CYB645 Cybersecurity Risk Analysis and Management* We have highlighted for the convenience of the EEC and CY.Q.A.A. with yellow highlights the additions and adjustments made on the respective syllabi (please see updated syllabi of all courses in Appendix I).	Choose level of compliance:
1.3 Finally, to properly cover training on the topic of *Incident Planning, Response, Forensics,* electives in “Threat Intelligence”, “Crisis Management/Communication” and “Leadership in High-Stress/Crisis Situations” would be worth exploring.	We thank the EEC for this insightful recommendation. In agreeing with this recommendation, we have added two new elective courses one on *Cyber Threat Intelligence (CYB660)* and one on *Management of Communication and Leadership in High Stress and Crisis Situations (CYB*665*).*	Choose level of compliance:

	The syllabi of both the new courses are available in Appendix I where you can find the updated syllabi for all courses. In addition, in Appendix II you may find the updated programme structure which mirrors these changes.	
1.4 In terms of the *programme structure*, the role of the Masters thesis is worth reconsidering. In part, according to the discussions during the site-visit, more than half of students opt for the electives rather than the thesis. Also, the evolution of cybersecurity as a scientific and professional domain means that the required core skill-set evolves and expands – making it valid to reassess the 'thesis option' or its delivery, for example by enhancing its independent research component.	We agree with the recommendation of the EEC to further enhance the programme's research component. We, therefore, have redesigned the *assessment methodology* of the courses *CYB635 Research Methods* and *CYB615 Cybersecurity Policy, Governance, Law and Compliance* which have now been enhanced with the implementation of research activities throughout their duration. Indicative examples of *research assessment activities* in the course *CYB635 Research Methods*: "This research project focuses on conducting a small-scale empirical study or a literature-based dissertation in the field of *a topic related to cybersecurity*. The primary emphasis of the dissertation will revolve around exploring the application of specific research methodologies to investigate relevant issues, examining their practical functionality, and incorporating research reflexivity throughout the process. The study will also aim to report on its findings, although considering the limited scale, the objectives will be modest to allow for a comprehensive methodological critique and potential methods development as an outcome." In addition, in the same course *CYB635 Research methods* course we enhanced its independent	Choose level of compliance:

	research component, through mentoring, collaborative opportunities, access to resources and emphasizing ethical considerations. Students will thus be able to gain valuable research skills and experiences. These enhancements foster a supportive and enriching environment that empowers students to conduct high-quality independent research and prepares them for future academic or professional endeavors. Similarly, Indicative examples in the course *CYB635 Cybersecurity Policy, Governance, Law and Compliance*: “Ensuring compliance with the incident notification requirements of the NIS2 Directive: Best practices and challenges for operators of essential services (OES) and digital service providers (DSPs).” Throughout this module, you have been introduced to the legal considerations associated with cybersecurity and how and why compliance is important. This topic aims to explore the requirements for incident notification under the NIS2 Directive, including the timeline for reporting incidents, the types of incidents that must be reported, and the information that must be included in incident reports. You are requested to examine the challenges that OES and DSPs may face in meeting these requirements, such as the need for effective incident response plans and communication protocols, as well as the potential consequences of non-compliance. Concluding, you need to discuss best practices for incident notification and compliance with the NIS2 Directive.”	

1.5 In terms of the programme documentation, the submitted materials list each course as granting 10 ECTS units – which corresponds to 250-300 study-hours. However each course is also listed as 42h of "lectures" (or equivalent) with, explicitly, "none" indicated for lab/exercises – rendering the question of how the students spend the balance of 200-250h of their "study time" per course. Discussions during the site visit suggests that perhaps the "lab/exercises" component was underestimated, and this merits therefore being clarified and properly documented.	We thank the EEC for their comment. As also admitted during the onsite visit, where the same comment was also discussed, it has been an oversight on our behalf not to mention the teaching methodology followed in our practical courses which include intense lab activity (which as the EEC validated the lab component is strongly eminent in all practical courses). In the course syllabi the field referring to laboratories has been adjusted for conventional practical courses. We have highlighted for the convenience of the EEC and CY.Q.A.A. with turquoise highlights the adjustments made and the total estimation of the lab hours on the respective syllabi (please see updated syllabi of all courses in Appendix I).	Choose level of compliance:
1.6 As for the programme organisation, given the significance of research for faculty promotion (*"substantial record of presentations at peer-reviewed conferences"*, *"substantial output in form of articles in refereed journals"*, *"strong participation in research grants or research projects"*, *"evidence of contribution to the research community"*, *"impact on an international level…indicated by citation impact analysis"*, etc, as per faculty promotion guidelines, *it is critical for staff retention – and, therefore, for the successful continuation of the programme* – to ensure conditions conducive to enabling the full-time faculty to: ● produce a substantial record of presentations	We thank the EEC for this recommendation. As discussed with the EEC, the conventional programme of study is not currently offered, thus no students are admitted. As soon as we re-offer the programme of study, we will consider recruiting more full-time academic staff.	Choose level of compliance:

at peer-reviewed conferences, and publications in refereed journals; • apply for and participate in research grants/projects; • demonstrate contributions and scientific impact on an international level. To this end, it is the EEC’s view that recruiting a senior faculty member with an international profile, relevant expertise, and ability to inspire and manage staff will contribute to a *renewal of the collective research dynamics in cybersecurity* within the existing team at EUC – in addition to sharing the teaching and administrative load involved in the delivery of the cybersecurity programmes.		
1.7 In terms of the *programme’s place and professional and academic prestige*, given that this is a “conventional” cybersecurity programme which is primarily geared for students seeking a Masters degree in Cybersecurity as their first professional degree co-exists and competes with the e-learning cybersecurity programme which is primarily targeting working professionals seeking to add “cybersecurity” to their existing professional competencies, it may be worthwhile considering the respective content of the two programmes.	We thank EEC for their comment. Indeed, offering the same content in both conventional and e-learning Masters in Cybersecurity might cancel each other out. Therefore, we have restructured the conventional Master in Cybersecurity to differ from the E-learning one. Please see our response in comment 1.8 below.	Choose level of compliance:
1.8 One option could be to concentrate only on the	In agreeing with the EEC and in continuation of the item 1.7 above, we	Choose level of compliance:

successful e-learning programme. A more ambitious option would be to position the two programmes differently. For example, for the “conventional” programme to explicitly position, label, and structure it as specialising in (with reference to the three topics discussed under “Program Content”) *“Systems construction”* and “*Incident Planning, Response, Forensics"* – and maintaining and further developing the innovative pedagogical activities that the faculty members and instructors are already promoting: “Capture the Flag” (CTF) competitions, Cyber-exercises, group projects, etc. This would also allow positioning, labelling, and structuring the e-learning programme explicitly for the target audience – working professionals, with both experience and with constrained calendars – for example by emphasising (with reference to the three topics discussed under “Program Content”) “*Audit, Governance*”, which necessitates a certain prior professional experience. This would also allow adapting the pedagogical approach, *e.g.,* avoiding synchronous group projects, not easy to fit into the schedules of working professionals, and emphasising, for example, case studies/analysis.	have restructured the conventional programme of study to explicitly position it differently than the E-learning one. 1. We introduced a different structure to the curriculum of programme, so that it encompasses the Committee’s suggestions and thus allow students to take more courses towards their M.Sc. in Cybersecurity under two specialisations (namely, ***Audit and Governance*** and ***Incident Planning, Response, and Forensics***). More specifically, the newly revised curriculum includes six (6) compulsory courses during the first two semesters. The course CYB615 Cybersecurity Policy, Governance, Law and Compliance, has now moved to the specialization of “Audit and Governance”, and was thus substituted in the compulsory course list by the course CYB640 Special Cybersecurity Topics. This course will allow the quickly evolving area of cybersecurity to be kept up to date with the latest trends and research in the field of cybersecurity being presented. In addition, during the third semester and taking EEC’s comments into consideration, we have structured the programme of study providing two specialisations: the students are required now to choose two (2) elective courses from one of the two new specializations offered. **Audit and Governance**, comprised out of the courses: *CYB645 Cybersecurity Risk Analysis and Management,* and *CYB615 Cybersecurity Policy, Governance Law and Compliance.*	

	And another specialisation on **Incident Planning, Response and Forensics**, comprised out of the courses: *CYB655 Incident Response and Forensic Analysis,* and *CYS660 Cyber Threat Intelligence.* Alternatively, during the third semester, the students can choose the CYB670 M.Sc. Thesis (30 ECTS) course, which (as recommended by the EEC) is now more enhanced with applied industrial research or placement. All the aforementioned changes are demonstrated in Appendix II, which presents the revised curriculum of the programme. We believe that with these changes the number of courses that students need to take is satisfactory and in this way it is ensured that students will be exposed to core Cybersecurity as well as to cutting-edge themes in the field of Cybersecurity, thus allowing them to obtain a M.Sc. in Cybersecurity with the most updated content. 2. In order to strengthen the programme’s quality, we changed the elective M.Sc. Thesis course “CYB670 Master Thesis”, so that the criteria set by the European Qualifications Framework are fully satisfied. Additionally, we have revised and enhanced the objectives and learning outcomes of its syllabus. Through the M.Sc. Thesis, students will actively participate in research and development of scientific work. Through this process, they are expected, among others, to demonstrate their ability to identify and formulate issues critically, independently and creatively, to undertake advanced tasks within	

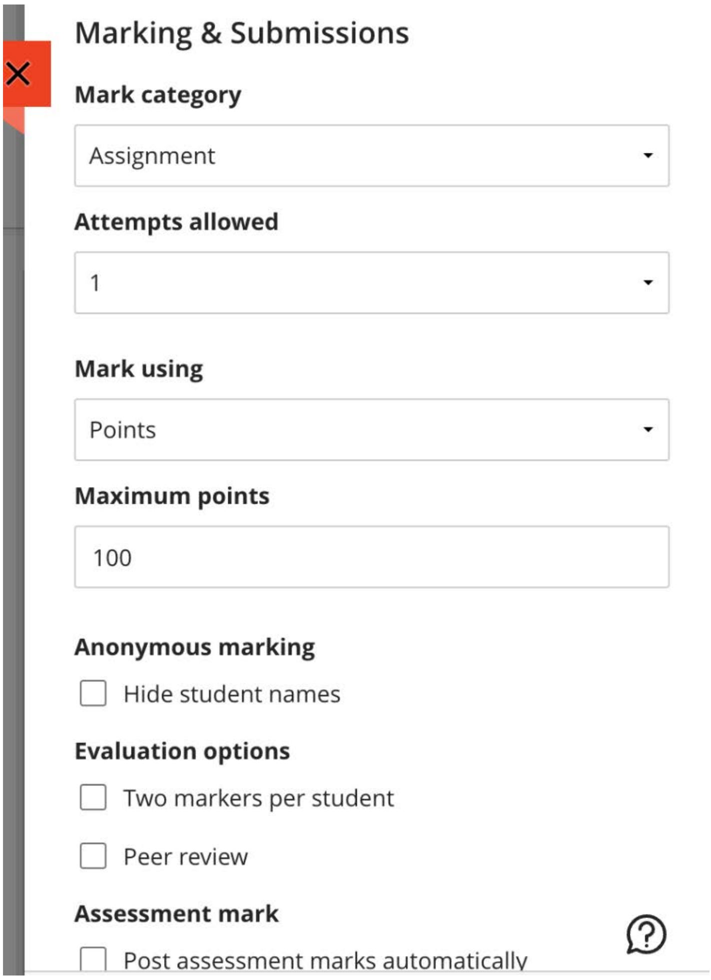
	predetermined timeframes, and to contribute to the formation of knowledge, as well as the ability to evaluate their work. Thus, students are now expected to design and perform original research work. We believe that these additions will further facilitate students' learning and promote their critical appraisal skills, collaboration, and creativity that are necessary for research and students' postgraduate education.	

2. Student – centred learning, teaching and assessment
(ESG 1.3)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
2.1 Consider using more open educational resources and open textbooks.	As discussed during the EEC's on-site visit, we are significantly using open education resources and open textbooks. We are also committed in continuously adding more and updating open educational resources and open textbooks in our courses. For example, in the course *CYB625 Ethical hacking and penetration testing* the instructor is mainly using OWASP, Merlot, MITRE and other open educational resources. Also, it would be useful to note that the Library subscribes to the Curriculum Builder Tool. The Tool is an add-on service for the Library's EBSCO Discovery Service (EDS) and part of the university's LMS platform Blackboard Learn Ultra. The Tool provides the faculty the option to search from within the LMS platform all the Library's paid services (such as databases, e-books and e-journals). Furthermore, it allows the Faculty to search online for any Open Educational Resources and Open Textbooks and then directly use them in their courses. Any material found (such as web links to archives, free primary sources, e.g. government documents, pamphlets, texts of laws, poems, literary works, book chapters, and so on) can then be used to create reading lists, be used for student assignments, etc.	Choose level of compliance:
2.2 In addition to participating in classes together, ways of enhancing the international experience of the students could be explored such as inviting more international experts and guest lecturers for interactions (internationalisation at home).	We have taken EEC's comment into consideration and we will be calling international experts to add their expertise through guest lectures. Till now, we have been inviting as guest lecturers mainly national experts, but also some international ones through the Erasmus mobility scheme. But indeed, interaction with international experts can expose students to a broader range of experiences and challenges faced in cybersecurity on a global scale, fostering a more comprehensive understanding of the subject matter. We will make sure to mobilise our international network and collaborations that are already established. We have thus already invited Huawei, in order to participate as guest lecturers in the course CYB600	Choose level of compliance:

	Introduction in Cybesecurity. Similarly, we aim to invite guest lecturers from renowened universities that we collaborate in research projects to provide lectures in various topics, to our students. Indicative examples are KU Leuven, University of Twente, Technical university of Brno, Universitad de Murcia.	
2.3 Increase the opportunities for research-oriented student learning (individual courses and thesis).	Please see our response in item 1.4 above where we have addressed this issue.	Choose level of compliance:
2.4 Increase the opportunities for practical training (individual courses or through placements).	Please see our response in point 1.8 above	Choose level of compliance:
2.5 Standardise assessment procedures across the program to ensure transparency, equality and fairness; for example by introducing second marking or moderation.	We thank the EEC for the opportunity to provide more information about this issue. The Department has in place a number of transparency, equality and fairness procedures regarding the assessment procedures across each of its programmes of study. Thus, it ensures that the examination and evaluation procedures are adhered to relevant practices based on the instructions of the Cyprus Agency of Quality Assurance in Higher Education (CY.Q.A.A.). For instance, the Department uses external examiners in assessing students' Master and Doctoral Thesis. In addition, based on the guidelines of CY.Q.A.A., the Department maintains final exams for a period of three years and also does a random sampling of all courses' assignments (Good-Average-Poor) and keep them for two years (see CY.Q.A.A. instruction: https://www.dipae.ac.cy/index.php/el/nea-ekdiloseis/anakoinoseis-el/126-apofaseis-21-synodos). In addition, course assignments and final exams are presented to external evaluation committees during quality assurance procedures conducted by the CY.Q.A.A. Additionally, to safeguard the quality assurance of assessment grading, the Programme follows the process of internal blind review of the 20% of the assignments and exams. It is noteworthy to point out	Choose level of compliance:

	here that within the framework of the University's 35-hour Professional Development Programme (Appendix V) which focuses on various aspects on teaching and learning, topics such as grading procedures and differentiation of grades, are offered every academic year. As far as the recommendation about an external examiner, the University already has the following procedures in place: • Each Program Coordinator is responsible for assuring the quality of midterm and final exams by reviewing the exam papers for all courses of the program. • An Appeal procedure allows any student who believes that the grade received in the Final Exam is different from what was expected, to ask for a re-evaluation of his/her final examination/project to a second examiner other than the original instructor. Before requesting a re-evaluation, the student must exhaust all possibilities of resolving the problem with the pertinent instructor first. If this does not lead to a resolution, the student may appeal against the Final Exam grade by filing a petition with the Office of the Registrar within four (4) weeks from the date the results are announced. The Registrar will forward a copy of the petition to the pertinent Chairperson of Department, who will first ascertain that no error was made by the instructor, and if so will assign an anonymous re-evaluation of the final examination/project to second examiner. In the case of major discrepancy between the instructor's evaluation and the re-evaluation that will require change of grade, the average of the two evaluations will be assigned as the final grade to the final examination/project. Changes of grades resulting from an appeal require the endorsement of the Dean of School. • During Fall 2020-Spring 2022, and due to the special pandemic restrictions, an ad-hoc Quality Assurance team consisting of three (3) members of the Department, offered to each instructor and each course feedback on the consistency of each exam paper according to the pertinent EUC framework and suggests possible amendments. Additionally, it should be noted that for the assessment of all Bachelor senior projects and Master Theses the	

<table>
<tr><td></td><td>Department’s policy dictates that a committee of two members reviews and gives feedback to the student.</td><td></td></tr>
<tr><td>2.6 Anonymise student assessments.</td><td>In Black Board Learn Ultra assignment settings, you may indicate that the instructor may mark the assignments anonymously. Please see picture below:

Marking &amp; Submissions
Mark category
Assignment
Attempts allowed
1
Mark using
Points
Maximum points
100
Anonymous marking
□ Hide student names
Evaluation options
□ Two markers per student
□ Peer review
Assessment mark
□ Post assessment marks automatically
From F2023, all instructors teaching in the Master in Cybersecurity will be using this functionality to anonymize students’ assessments.</td><td>Choose level of compliance:</td></tr>
<tr><td>2.7 Introduce program and course specific grade descriptors.</td><td>In all course outlines, there is a section dedicated on the grading system used at the European University Cyprus. You may find this below:
<table>
<tr><td><b>GRADING SYSTEM:</b></td></tr>
<tr><td><b>GRADUATE</b></td></tr>
</table>
<table>
<tr><th>Letter Grade</th><th>Grade Meaning</th><th>Grade Points</th><th>Percentage Grade</th></tr>
<tr><td>A</td><td>Excellent</td><td>4.0</td><td>90 and above</td></tr>
</table></td><td>Choose level of compliance:</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>B+</td><td>Very Good</td><td>3.5</td><td>85-89</td><td></td></tr>
<tr><td>B</td><td>Good</td><td>3.0</td><td>80-84</td><td></td></tr>
<tr><td>C+</td><td>Above Average</td><td>2.5</td><td>75-79</td><td></td></tr>
<tr><td>C</td><td>Average</td><td>2.0</td><td>70-74</td><td></td></tr>
<tr><td colspan="4"></td><td></td></tr>
<tr><td>F</td><td>Failure</td><td>0</td><td></td><td></td></tr>
<tr><td>I</td><td>Incomplete</td><td>0</td><td></td><td></td></tr>
<tr><td>W</td><td>Withdrawal</td><td>0</td><td></td><td></td></tr>
<tr><td>P</td><td>Pass</td><td>0</td><td></td><td></td></tr>
<tr><td>AU</td><td>Audit</td><td>0</td><td></td><td></td></tr>
</table>
(a) The grade "I" is awarded to a student who has maintained satisfactory performance in a course but was unable to complete a major portion of course work (e.g. assignment/paper or final exam) and the reasons given are acceptable to the instructor. It is the responsibility of the student to bring pertinent information to the instructor to justify the reasons for the missing work and to reach an agreement on the means by which the remaining course requirements will be satisfied. A student is responsible, after consulting with the instructor, for fulfilling the remaining course requirements within the first four weeks of the following semester for which an "I was awarded. In very special cases, the instructor may extend the existing incomplete grade to the next semester. Failure of the student to complete work within this specific time-limit will result in an "F" which will be recorded as the final grade.
(b) The grade "W" indicates withdrawal from the course before the specified time as explained in the withdrawal policy.
(c) Grades of "P" will not be computed into a student's cumulative grade point average but will count towards graduation credits.
(d) Grades of "F" will be computed into the student's cumulative grade point average.
(e) Students enrolling for an Audit must designate their intent to enrol on an Audit basis at the time of registration. Students registering for a course on an Audit basis receive no credit.

This is also presented on the EUC website under here.
</td>
<td></td>
</tr>
<tr>
<td>2.8 Introduce (if they do not already exist) processes to deal</td>
<td>Students receive detailed feedback on the parts that are submitted towards the completion of their course requirements in a timely manner. Where a student</td>
<td>Choose level of compliance:</td>
</tr>
</table>

<table>
<tr>
<td>with student complaints about grades.</td>
<td>disagrees with an exam grade awarded, he/she must exhaust all possibilities of resolving the problem with the course Instructor. In the event that no agreement is reached, the student may appeal by filing a petition with the Office of the Registrar, within four (4) weeks of the exam grade being awarded. The Registrar will forward a copy of the petition to the pertinent Chairperson of Department, who will first ascertain that no error was made by the instructor, and if so will assign an anonymous re-evaluation of the final examination/project to second examiner. In the case of major discrepancy between the instructor's evaluation and the re-evaluation that will require change of grade, the average of the two evaluations will be assigned as the final grade to the final examination/project. Changes of grades resulting from an appeal require the endorsement of the Dean of School. Details of this process as noted in the University Charter (please see EUC Charter: Annex 2: Internal Regulations on Students' Admission, Evaluation, Advancement And Graduation; here). This is also presented on the EUC website under here.</td>
<td></td>
</tr>
<tr>
<td>2.9 Establish and communicate submission deadlines for assignments and homework at the beginning of the academic year, and communicate dates for submission and release of grades with additional lead-time.</td>
<td>In all course outlines shared with students for every course at the beginning of the academic semester, there is a weekly breakdown that indicates the exact submission deadlines for assignments and homework. See for example the following extract from CYS600 – Introduction in Cybersecurity.
<table>
<tr><th colspan="2">WEEKLY BREAKDOWN (excluding Christmas or Easter Holidays):</th></tr>
<tr><th>WEEK</th><th>TOPIC</th></tr>
<tr><td><b>1</b></td><td>Week 1 - Cybersecurity, Network and Information Security</td></tr>
<tr><td><b>2</b></td><td>Week 2 - Introduction to Information Security</td></tr>
<tr><td><b>3</b></td><td>Week 3 - Information Security Policy
<b>Assignment 1 – Deadline in Week 5</b></td></tr>
<tr><td><b>4</b></td><td>Week 4 - Information Security Governance</td></tr>
<tr><td><b>5</b></td><td>Week 5 - Risk Management: Identifying and Assessing Risk</td></tr>
<tr><td><b>6</b></td><td>Week 6 - Compliance: Auditing, Monitoring, and Logging
<b>Assignment 2 – Deadline in Week 8</b></td></tr>
<tr><td><b>7</b></td><td>Week 7 – Invited lecture</td></tr>
<tr><td><b>8</b></td><td>Week 8 - Planning for Contingencies</td></tr>
<tr><td><b>9</b></td><td>Week 9 - Information Security Maintenance</td></tr>
</table>
</td>
<td>Choose level of compliance:</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td><b>10</b></td><td>Week 10 - Legal and Regulatory Requirements
<b>Assignment 3 – Deadline in Week 12</b></td></tr>
<tr><td><b>11</b></td><td>Week 11 - Cyber Law</td></tr>
<tr><td><b>12</b></td><td>Week 12 - General Data Protection Regulation (GDPR)</td></tr>
<tr><td><b>13</b></td><td>Revision Week and Final Examination</td></tr>
<tr><td><b>14</b></td><td><b>FINAL EXAMS
(the final examination will be with closed books)</b></td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>2.10 Revisit assessment methods to suit this type of program although we acknowledge that this should involve the relevant educational authorities in Cyprus.</td>
<td>Assessment methods for all programmes of study are in line with the CY.Q.A.A. guidelines. In more specific, throughout the programme there is class participation and attendance marked with 10% to comply with the national regulation where attendance in conventional programmes is compulsory. Then, there is a 70% dedicated to the examinations including the midterm and final examination of each course. In practical courses like the CYB625 Ethical Hacking and Penetration Testing and CYSB655 Incident Response and Forensic Analysis, both midterm and final examinations are split in two parts, namely practical and theoretical. This is actually required due to the nature of the programme of study and the context of such practical courses. This mode of assessment is applied in all new practical courses introduced due to the changes as per EEC's comments, e.g. the CYB660 Cyber Threat Intelligence course (please see our response in points 1.3. and 1.8). Finally, there is a 20% of the total grade assigned to assignments, that according to the nature of each course are tailored to meet the learning objectives. For example, in the cases of practical courses, all assignments are hands-on laboratory assignments, where students need to apply their acquired practical knowledge. In the cases of theoretical courses like CYB615 Cybersecurity Policy, Governance, Law and Compliance and CYB645 Cybersecurity Risk Analysis and Management, the assignments are theoretically based and include research perspectives as well (please see our response in point 1.4)</td>
<td>Choose level of compliance:</td>
</tr>
</table>

3. Teaching staff

(ESG 1.5)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
3.1 Recruit more staff and, as stated earlier, senior staff with an international research profile.	Please see our response in item 1.7 above where we have addressed this issue.	Choose level of compliance:
3.2 Align internal staff evaluation processes with the promotion process. This contributes to transparency, staff integration and retention.	As discussed during the EEC's on-site visit, there is a Faculty Performance Appraisal procedure in place (please find the relevant Internal Regulation in Appendix III), as well as a clear, transparent promotion process as indicated in the University Charter (please see Annex 6 – Chapter 5, pp. 74 - 80 in EUC charter here). Even though these two processes are distinct, for Faculty promotion, the Faculty Performance Appraisal is one of the data sources evaluated by promotions committees for their decision on the promotion of a Faculty applicant. In more specific, the Faculty Performance Appraisal document of the years between the previous promotion of the Faculty and the one in evaluation is taken into consideration for the promotion criteria as follows: -Positive and substantial evidence of high competency in teaching; -Research and scholarly publications or recognized creative work in the individual's field; and -Evidence of service to the University and Community in general.	Choose level of compliance:

	This provides a clear and transparent link between the two procedures, aiming at the enhancement of staff performance and align it with the promotion process. The expectation and standards for promotion are clearly communicated to all staff members, thus ensuring that staff are aware of the factors considered during evaluations and understand what is required for career advancement.	
3.3 Align workload with internal staff assessment and promotion processes	We thank EEC for this comment. The proposed change requires change in the EUC charter, which involves changes outside the scope of the programme as such. The EEC recommendation has been submitted to the Rectorate Committee for their consideration.	Choose level of compliance:
3.4 Introduce performance targets and performance monitoring.	In continuation to our response in item 3.2 above, performance targets are clearly stated for each separate rank in the description of the expectations of faculty ranks (Lecturer, Assistant Professor, Associate Professor, Professor) as described in the University Charter (please see Annex 6 – Chapter 2 – Faculty Ranking, pp. 70 in EUC charter here), as well as the expectations for promotion from one rank to the other. Individual performance targets and performance monitoring is achieved as follows: 1. through the Performance Appraisal procedure (please find the relevant Internal Regulation in Appendix III).	Choose level of compliance:

	2. the Department implements a mentorship scheme, called "EUC Framework on Mentoring Scheme for Newly Hired Full-Time Academic Staff and/or Part-Time Academic Staff" under which, newly hired faculty members with less academic experience have the opportunity to work and learn from more senior colleagues. The scheme appears in Appendix IV.	
3.5 Introduce School wide mechanisms to assess the quality of research outputs from mentoring to post publication assessment.	In accordance with the EEC, members of our Department are implementing a mentoring scheme, where junior faculty are being mentored in grant proposal writing by more experienced faculty and researchers. For example, the senior Faculty member Professor George Boustras Founder and Director of CERIDES – Excellence in Innovation and Technology center, together with junior Faculty member Dr Cleo Varianou-Mikellidou (Lecturer) work on submitting various European funded research proposals. Similarly, senior Faculty member Dr. Christos Dimopoulos (Associate Professor) Co-founder of CERIDES together with junior Faculty member Dr Pericles Leng Cheng (Lecturer). Moreover, the EUC Research Office regularly organizes seminars and workshops for the academic faculty concerning proposal writing, funding opportunities, and other issues pertaining to research, such as	Choose level of compliance:

	open science, research ethics, project administration and data management. In addition, the Research Office informs faculty members via email communication about upcoming calls for proposals announced by the European Commission, the National Research and Innovation Foundation and other funding bodies tailored to the different disciplines and areas of focus. Finally, the Department implements a mentorship scheme, called “EUC Framework on Mentoring Scheme for Newly Hired Full-Time Academic Staff and/or Part-Time Academic Staff” under which, newly hired faculty members with little experience in funded research have the opportunity to work and learn from more senior colleagues. The scheme appears in Appendix IV.	
3.6 Lay down clear rules about working hours, response times and communicate them to staff and students.	At EUC, conventional students receive continuous academic support. All members of academic staff obligatory assign six (6) hours of Office Hours every week for consultation and support to students. Students are thus encouraged and advised to make use of these office hours as an important academic support structure in place that provides direct, personal and personalized contact with course instructors. The University has also an established policy for re-scheduling office hours. In addition, the instructor, who guides students for effective self-study, employs a range of alternative methods to increase	Choose level of compliance:

	his/her Office Hours contact time and effectiveness. Considerable contact time is devoted to students in discussion forums and through emails, through one-to-one meetings aiming at addressing customised needs of individual student needs (either on campus or through teleconferneces). As the EEC alerts, there is a risk of abuse of the academic staff working hours and at the same time, if -as the EEC points out-clear rules are not laid down about working hours and response times and not being communicated to students, no expectations from both sides could be valid. Therefore, the Office Hours to be held by each faculty member are listed in the course outline of the taught course. The course outline is shared with students in the BB page of each course. Please see Appendix V.	
3.7 As most of the teaching in the cybersecurity programme is done by adjunct part-time faculty (scientific collaborators), it is important to provide them with professional development opportunities.	EUC is committed to its academic staff professional development. The Faculty Professional Development C.I.Q.A. Standing Committee sets up a series of annual trainings which is provided to the teaching staff, both as initial training and as on-going training. Thus, EUC provides constant pedagogical and technological support to academic staff through the Faculty Professional Development Program. The Professional Development Programme ensures a high-level quality of teaching and the familiarization of all teaching personnel with contemporary	Choose level of compliance:

	pedagogical approaches and methodologies as well as technological and technical innovations. All professional development opportunities that are given to full time academic staff, as also given to part-time faculty through the Faculty Professional Development (FPD) scheme. Please find attached the 2022-2023 FPD full programme (Appendix VI).	
3.8 The programme is taught by 2 full-time faculty members, assisted by 4 part-time adjunct instructors. Even with the upcoming recruitment of a 3rd full-time faculty member, that still means that the programme has more visiting staff members than faculty members.	We have taken EEC's comment into consideration, and we are now in the process of hiring a high-profile academic staff in the area of cybersecurity. In addition to comment 1.6 above, we would like to underline that the conventional programme of study is not currently offered and thus there is not teaching load for staff members.	Choose level of compliance:

4. Student admission, progression, recognition and certification
(ESG 1.4)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
Click or tap here to enter text.	No recommendations by the EEC applied in this section. We thank the EEC for its positive recommendations.	Choose level of compliance:

5. Learning resources and student support
(ESG 1.6)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
5.1 Introduce specific student oriented well-being and mental health services.	The European University Cyprus has as a top priority to keep our students, faculty and staff healthy and safe. Taking into consideration that mental health is an integral part of our overall wellbeing, our experts from the Center of Applied Psychology and Personal Development (KEPSYPA), offer their support to all our University's community. The Center aims to provide psychological and counselling services to all members of EUC (please see Appendix VII for the Center's provisions). At the same time, EUC administrative services are always available to support faculty and staff and ensure that students will receive the maximum service in order to fulfil their academic obligations as planned.	Choose level of compliance:
5.2 Provide well-being and mental health training to academic staff, in particular to program directors.	In the same Appendix VI, you may find the section named "**Context and Services**" (please see 10. Training seminars to EUC staff on psychology topics; and 11. Seminars for personal development and prevention of mental health problems). Additionally, KEPSYPA has scheduled an upcoming training for programme coordinators in September 2023.	Choose level of compliance:

5.3 It was observed during our on-site visit that the Computer Labs have 20 to 35 students' capacity with only one door-level exit. EUC should ensure that classrooms, labs and other facilities are compliant with the Health and Safety regulations.	The EU Health and Safety Regulations and the International Building Code (IBC) allow one exit or exit access doorway in educational spaces including the computer labs, in which: 1. The maximum occupant load is 49 people. 2. The maximum common path of egress travel distance does not exceed the 22.5 meters. 3. There is not a sprinkler system in place. Only specific labs with chemical and infectious substances and LPG provisions are excluded from the above requirements. These regulations are featured at the ***Table 1006.2.1*** in ***Chapter 10 – Means of Egress*** (page 6 of the chapter) of the IBC. In addition, the ***Chapter 3 – Occupancy classification and use*** of the IBC defines that the educational spaces refers to Group E classifications and incudes the Higher Education buildings.	Choose level of compliance:
5.4 EUC should lead by example by not using single passwords for all their computers, and not publishing said passwords on placards on the walls of the computer labs.	In EUC, information security is viewed very seriously. Students use their username and password when using any EUC computer lab. The common username and password noticed by the EEC, is only used when it is necessary to use software that is licensed specifically for a specific lab. In this case, the account is a modified user local account without any network	Choose level of compliance:

	and administrative permissions. In addition, to further address the concerns of the EEC, we will take the following corrective measures: • we will update the student profiles to include the specific software when using the specific lab • a setup of the migration has been planned and will be completed before the start of the new academic year.	

6. Additional for doctoral programmes

(ALL ESG)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
N/A	Click or tap here to enter text.	Choose level of compliance:

7. Eligibility (Joint programme)

(ALL ESG)

Areas of improvement and recommendations **by EEC**	Actions Taken by the Institution	For Official Use ONLY
N/A	Click or tap here to enter text.	Choose level of compliance:

A. Conclusions and final remarks

Conclusions and final remarks **by EEC**	Actions Taken by the Institution	For Official Use ONLY
The program provides core knowledge and skills on cybersecurity, an area of ever increasing scientific and professional interest. It is delivered by committed staff. It follows University policies on admission, teaching and assessment. The library and technical resources are very good and support the delivery of the program. Student satisfaction is high. Graduates work in the public and private sector. In sum, it is a program which responds to current needs and has the potential for growth. During the on-site visit, teaching staff and members of the University administration were cooperative and ready to respond to our questions and provide the requested information. Our report and specific recommendations cover all relevant areas (design, delivery, teaching and assessment, staff, resources) with a view of enhancing the potential of the program. We are very much encouraged by the School's response to the previous assessment and remain at the disposal of the School if they need further information or clarifications.	We sincerely thank the EEC for the positive feedback and its constructive recommendations. We found the EEC's candid discussions a constructive learning process as we were provided with critical input on moving forward effectively. We have thoroughly reviewed the findings, strengths, and areas of improvement indicated by the EEC following its review and addressed all comments in full. By embracing the EEC's comments and suggestions, we are convinced that our program will effectively ensure its students' learning outcomes. As identified by the EEC, the quality of the programme and the student-faculty relationship is closely monitored and we intend to maintain and further enhance this successful interaction between our faculty and our students. Overall, we have complied with the suggestions made by the EEC. In sum, we have enriched our syllabi with elements on Systems Construction, Audit, Governance, and Incident Planning, Response, Forensics as described in the EEC's comments (please see our responses in items 1.1 – 1.8). In addition, we have clarified the hours that in practical courses, there is significant time allocated in labs/exercises. Finally, we have added aligned internal staff	Choose level of compliance:

	evaluation processes with the promotion process (please see our response in item 3.2). Moreover, we have redesigned the Master in Cybersecurity (conventional) to differ from the Master in Cybersecurity (e-learning). In closing, we are grateful to the EEC for their suggestions and insightful comments with regard to the Master in Cybersecurity conventional programme.	

B. Higher Education Institution academic representatives

Name	***Position***	***Signature***
Dr. Yianna Danidou	Program Coordinator	
Dr. Ioannis Michos	Chairperson, Department of Computer Science and Engineering	
Prof. Panagiotis Papageorgis	Dean, School of Sciences	

Date: 7.8.2023

European University Cyprus

Appendix I

Course Title	Introduction to Cybersecurity				
Course Code	CYB600				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	Dr Ioanna Danidou				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental concepts and terminology of cybersecurity as a whole, and functions as a short introduction to the large number of cybersecurity topics that are covered within this MSc programme.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the meaning and position of fundamental cybersecurity concepts and terminology • Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model • Classify and describe different cybersecurity components and how they contribute to effective defence • Classify and describe different potential routes for cyber attacks. • Recognise the importance and application of IT law and cybersecurity certification				
Prerequisites	None	Co-requisites	None		

Course Content	Introduction: Refresh on fundamental networking principles and devices and distributed systems, the context within which cybersecurity (or lack thereof) can be present. Network structure and ways of communication. History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.) Current importance of cybersecurity, given the connectedness of most of our daily lives. Analysis of critical infrastructures and the position of critical information infrastructures within these – importance of the protection of such systems for the smooth operation of essential services in all areas of life. The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Asset protection (including data) as a valuable business operation and its contribution to business survivability. Main principles of cybersecurity – confidentiality, integrity, availability and combinations thereof, resulting in other important cybersecurity concepts and services – accountability, non-repudiation, authenticity, resilience, business continuity and disaster recovery, audit, cybercrime, data / system / network forensics, cyberdefence. Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover. Incident response and forensics -_the incident response lifecycle stages, develop an effective incident response plan, understanding of incident detection, containment, and basic remediation techniques, digital forensics principles, forensic tools and techniques, and legal and ethical considerations in incident investigations. Applicable cybersecurity and IT law Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust. Introduction to ISO/IEC 27001 Information security management. Introduction to other courses in this MSc (to aid selection of the elective courses). Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.

Teaching Methodology	Face – to – face
Bibliography	*“Introduction to Computer Networks and Cybersecurity”,* by Chwan-Hwa (John) Wu and J. David Irwin *“Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover”*, by Lee Mark Zeichner “Management of Information Security” by Michael E. Whitman, Herbert J. Mattord “CISSP Guide to Security Essentials” By Peter Gregory “Principles of Information Security” by Michael E. Whitman, Herbert J. Mattord *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines* (ISC)^2, ISACA, and other cybersecurity websites
Assessment	Class participation and attendance: 10% Examinations: 70% Assignments: 20% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Communications and Network Security</td></tr>
<tr><td>Course Code</td><td colspan="5">CYB605</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 1st Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">TBA</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/10 weeks</td><td>Laboratories / week</td><td>3 hours/4 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces fundamental concepts of communications and network security, particularly in the context of internal and external threats to the operation of the network and to the devices that are attached to it.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, and separation of duties.
• Explain the basic types of networking device, both logical and physical.
• Differentiate between the various properties of security as they relate to the design of authentication protocols and the use of asymmetric and symmetric cryptography
• Classify and describe the different types of malware, network vulnerabilities and attacks.
• Classify and describe different types of wireless network attacks including sensor networks and Internet of Things (IoT)
• Describe and evaluate methods and devices used to protect networks.
• Compare security mechanisms of Cloud Computing
• Describe the key issues when managing emergencies</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>CYB600</td></tr>
<tr><td>Course Content</td><td colspan="5">Introduction: Refresh on fundamental networking principles and devices, OSI and TCP/IP models. Different types of networking areas – WAN, LAN, MAN, PAN, wireless and mobile systems.
Security Principles: Security Properties, the network as a route for cyberattacks, types of attacks, security mechanisms and services.</td></tr>
</table>

	Threats and Attacks: Threats and vulnerabilities, hardware vs. software vulnerabilities, social engineering, malware types, Network attacks: scanning, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-middle, session takeover, ARP poisoning, ICMP attacks, DNS poisoning, phishing, spam, Security protocols at the various OSI layers: TLS, SSL, IPsec, authentication protocol design based on Asymmetric and Symmetric encryption, Security properties of symmetric and asymmetric encryption, digital signature properties Wireless Network Security: Encryption and key management vulnerabilities, wireless sniffing, war-driving, mobile/cellular cell spoofing, eavesdropping, wireless sensors security, routing attacks, IoT security Cloud security - definitions pertinent to cloud computing, identify risks, and delve into a security architecture, data protection, access management, monitoring, compliance, and emerging trends. General protection, prevention and detection: Firewalls and packet filtering, demilitarized zones (DMZ), intrusion detection and prevention systems, IPsec, VLANs and network zoning, authentication, system hardening, encryption, authentication, , honeypots , Cloud computing Disaster and Risk Management: Managing emergencies, factors for quick disaster response Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*" Computer Networking: A Top-Down Approach (7th Edition), by Jim Kurose and Keith Ross.* *"Guide to Computer Network Security, 4th Edition", by Joseph Migga Kizza* *"Network Security Essentials: Applications and Standards", Sixth Edition, by William Stallings* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*

Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Cryptography</td></tr>
<tr><td>Course Code</td><td colspan="5">CYB610</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 1st Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Dr Nicos Tsalis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/13 weeks</td><td>Laboratories / week</td><td>3 hours/2 weeks</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces fundamental concepts of cryptography and its uses in cyber and information security. Beyond the basic uses for keeping information secret and the different methods available, additional forms, such as hashes, digital signatures, non-repudiation and steganography, are introduced.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon succesful completion of this course students should be able to:
- Describe the underlying principles of cryptography, clear text, plain text, algorithms, and keys.
- Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them.
- Classify and describe a number of different encryption algorithms and the way that they work.
- Describe the mathematical principles behind encryption and the mathematical properties of ciphertext.
- Describe and evaluate different methods used to crack encryption.
- Explain the different uses of encryption methods and the security objectives that they meet.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td colspan="2">Co-requisites</td><td>CYB600</td></tr>
</table>

Course Content	Introduction: History of cryptography, early forms, cryptosystem strength, Caesar cipher, one time pad, steganography. Principles: basic cryptographic functions – substitution ciphers and transposition ciphers, symmetric and asymmetric algorithms, block and stream ciphers, hybrid systems. Symmetric systems: DES, 3-DES, AES, IDEA, Blowfish, RC4-5-6, Twofish, Serpent, others, uses and cryptographic services provided. Asymmetric systems: Diffie-Hellman algorithm, RSA, El Gamal, Elliptic Curve systems, zero knowledge proof, SSL/TLS, PGP, S/MIME, Bitcoin. Public key systems: one-way algorithms, public and private keys, public key infrastructure, certificate and trust authorities, distributed trust systems. Other cryptographic services: message and file integrity, hashing, digital certificates, digital signatures, key management. Attacks: known and chosen plaintext attacks, ciphertext attacks, analytical attacks, frequency analysis, statistical attacks, social engineering attacks. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the uses of cryptography in real systems.
Teaching Methodology	Face – to – face
Bibliography	*“Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series)”*, by Jonathan Katz and Yehuda Lindell *“Understanding Cryptography: A Textbook for Students and Practitioners”*, by Christof Paar and Jan Pelzl *“Applied Cryptography: Protocols, Algorithms and Source Code”*, by Bruce Schneier *“Modern Cryptanalysis: Techniques for Advanced Code Breaking”*, by Christopher Swenson *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*

Assessment	Class participation and attendance	10%
	Examinations	70%
	Assignments	20%
		100%
Language	English	

<table>
<tr><td>Course Title</td><td colspan="5">Cybersecurity Architecture and Operations</td></tr>
<tr><td>Course Code</td><td colspan="5">CYB620</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">1st Year / 2nd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Dr Nicos Tsalis</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>3 hours/14 weeks</td><td>Laboratories / week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This course introduces the fundamental security principles of confidentiality, integrity, availability, as well as related security services such as accountability, non-repudiation, authentication, etc. The whole operational environment is described, with reference to ongoing security processes such as user provisioning, vulnerability management, penetration testing, exercising, change management, incident response, risk assessment and others. The five phases of cybersecurity are discussed here – Identify, Protect, Detect, Respond, Recover.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon succesful completion of this course students should be able to:
• Identify the various components of a comprehensive cybersecurity architecture within an organization.
• Describe and classify controls that meet specific control objectives and to treat identified risks.
• Explain in detail the basic security principles of confidentiality, integrity and availability, as well as related security services such as accountability, non-repudiation, authentication, etc.
• Describe the five phases of cybersecurity operations: Identify, Protect, Detect, Respond, Recover.
• Describe and evaluate the processes of vulnerability management, penetration testing, exercising, change management, incident response, and others.
• Classify and describe a number of different effects of main cybersecurity controls on the operational environment, e.g. access control.
• Evaluate and select appropriate architectural and operational options according to the organizational risk environment.</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td>Co-requisites</td><td colspan="2">CYB600</td></tr>
</table>

Course Content	Introduction: Definition of security objectives: confidentiality, integrity, availability, accountability non-repudiation, authentication. Processes: User provisioning, access control, vulnerability management, penetration testing, exercising, change management, incident response, others. Phases: Phases of cybersecurity operations, in relation to the before and after of an incident: Identify, Protect, Detect, Respond, Recover. Identify: Identification of organizational assets, threats, vulnerabilities and risks (details in risk assessment course), vulnerability management (open databases, CVE, etc.) as an essential process. Protect: Selection and evaluation of controls to meet control objectives and risks identified, application and monitoring of controls, control lists (ISO 27002, COBIT 5, SANS 20 Critical Controls, Australia DSD Top Mitigations, etc), defense-in-depth considerations, penetration testing, BCP and DRP testing, system hardening. Detect: Detection of cybersecurity incidents as they occur, evaluation of impacts, log analysis, IDS/IPS, attack vector analysis, SIEM (security incident and event management), indicators of compromise (IOC). Respond: Incident triage and response, CERT/CSIRTs, triggering and implementation of business continuity and disaster recovery plans, corrective controls. Recover: Orderly and planned return to prior operational status and capabilities, lessons learned, evaluation of corrective controls and supporting processes. Specific cybersecurity operations topics: Database security, secure software development, mechanisms for ensuring the security of information at rest, in transit, and during processing, side-channel considerations. DevSecOps: Core principles and benefits of DevSecOps, challenges of traditional software development and how DevSecOps addresses them, Integrating Security into CI/CD Pipelines, Implementing security checkpoints in continuous integration and continuous deployment (CI/CD) pipelines, Incorporating security testing, code analysis, and vulnerability scanning, Secure Code Practices, Threat Modeling in DevSecOps. Overview of popular DevSecOps tools and frameworks. Hands-on experience with selected tools for vulnerability assessment and security automation. Embedded Systems Security: basics of embedded systems and their applications, Identifying the security challenges specific to embedded

	devices, Embedded Systems Architecture, Exploring the architecture of embedded systems and potential vulnerabilities, Analyzing common attack vectors against embedded devices, Secure Boot and Firmware Protection, Implementing secure boot mechanisms to ensure the integrity of firmware, Exploring techniques for protecting firmware from unauthorized modifications, Communication Security in Embedded Systems, Integrating security into the embedded system development lifecycle, Performing security testing, including penetration testing and code reviews. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities of cybersecurity operations in real environments.
Teaching Methodology	Face – to – face
Bibliography	*Farwell, J.P., Roddy, V.N., Chalker, Y. and Elkins, G.C. The Architecture of Cybersecurity: How General Counsel, Executives, and Boards of Directors Can Protect Their Information Assets. University of Louisiana at Lafayette.* *Santos, O., Developing Cybersecurity Programs and Policies. Pearson.* *"Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare", by Thomas A. Johnson (Editor)* *"The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)", by Anne Kohnke and Dan Shoemaker* *ISO 27002:2013 - Information technology – Security techniques – Code of practice for information security management* *ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements* *Contreras, J., 2013. Developing a Framework to Improve Critical Infrastructure Cybersecurity (Response to NIST Request for Information Docket No. 130208119-3119-01). SSRN Electronic Journal.* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*

Assessment	Class participation and attendance	10%
	Examinations	70%
	Assignments	20%
		100%
Language	English	

Course Title	Ethical Hacking and Penetration Testing				
Course Code	CYB625				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Dr Konstantinos Vavousis				
ECTS	10	Lectures / week	1 hours/14 weeks	Laboratories / week	2 hours/14 weeks
Course Purpose and Objectives	The objective of this course is to provide a detailed introduction into the world of ethical hacking and to understand its usefulness to organizations in practical terms. Hacking concepts, tools and techniques, and countermeasures are covered, along with how penetration testing fits into a comprehensive cybersecurity regime. Beyond the confines of ethical hacking, this course covers aggressive hacking techniques that are essential knowledge for professionals who need to be able to defend against such advanced attacks.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Define the different types of hacking and its legal and illegal uses in the cybersecurity world • Identify and evaluate the different type of hacking attacks and how these attacks proceed • Explain the principles of vulnerability research • Describe the different phases of ethical hacking and select appropriate techniques depending on the assignment. • Define, describe and perform the different kinds of penetration testing – black box, grey box, white box. • Make effective use of penetration testing related tools • Define which tool is more effective at each step of a penetration testing project				
Prerequisites	None	Co-requisites	CYB600		

Course Content	Introduction: Definition of ethical hacking and penetration testing, position within a comprehensive cybersecurity posture, applicable national and international laws, difference between ethical (white hat), non-ethical (black hat) and grey hat hackers, vulnerability research and zero-day vulnerabilities. Hacking phases: The five phases of hacking – reconnaissance, scanning, gaining access, maintaining access, covering tracks. Reconaissance: Discovery of target information, footprinting, competitive intelligence, social engineering, Google hacking, website footprinting, email tracking Scanning: TCP flags, ping sweeps, connect scans, TCP flag manipulation, SYN scans, IDLE scans, scanning tools, banner grabbing, vulnerability scanning, ip spoofing, enumeration techniques and tools Gaining and maintaining access: password cracking, dictionary attacks, brute force attacks, hashing attacks, privilege escalation, executing applications, malware (viruses, worms, trojans, rootkits, spyware, botnets), lalware detection and anti-malware software, DoS/DDoS, network sniffing, MAC, ARP and DNS attacks, session hijacking, web application attacks, SQL injection, wireless network and mobile device attacks, cryptanalysis and related attacks. Covering tracks: Rootkits, disabling auditing, clearing logs, anonymisers, proxies, hiding files, track covering tools Practical penetration testing: Penetration testing methodology, ethical considerations, assignments and contracts, reporting, relationship to audits and audit techniques. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practicalities and challenges of penetration testing.
Teaching Methodology	Face – to – face
Bibliography	*Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing.* *Harper, A., Regalado, D., Linn, R., Sims, S., Spasojevic, B., Martinez, L., Baucom, M., Eagle, C., & Harris, S. (2018). Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition (5th ed.). McGraw-Hill Education.* *Gaia, J., Ramamurthy, B., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X. and Yoo, C., 2020, January. Psychological Profiling of*

<table>
<tr><td></td><td><i>Hacking Potential. In Proceedings of the 53rd Hawaii International Conference on System Sciences.</i>

<i>“Hacking: The Art of Exploitation, 2nd Edition”, by Jon Erickson</i>

<i>“Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson</i>

<i>IEEE/ ACM/ Elsevier/ Springer Journals and Magazines</i></td></tr>
<tr><td>Assessment</td><td><table>
<tr><td>Class participation and attendance</td><td>10%</td></tr>
<tr><td>Examinations</td><td>70%</td></tr>
<tr><td>Assignments</td><td>20%</td></tr>
<tr><td></td><td>100%</td></tr>
</table></td></tr>
<tr><td>Language</td><td>English</td></tr>
</table>

Course Title	Special Cybersecurity Topics				
Course Code	CYB640				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Dr Nicos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide the student with a comprehensive view of the current state of cybersecurity – major incidents and statistics, recent developments in law, policies, national and European strategies, privacy considerations, new technologies, Safer Internet and the various related professional certifications that are available. Also to provide insight from the organizations and a market perspective of cybersecurity as a critical factor of business growth and economic development. Finally to present the emerging cybersecurity ecosystem and need to keep up to technological developments and threats.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify and define the current events in cybersecurity • Describe the various statistics available on cybersecurity and successful attacks around the world • Explain recent developments in national, European and international cybersecurity laws and policies • Define and describe recent developments in the European area and the impact that these may have on the way cybersecurity operations are conducted • Define and describe the different parts of national and European cybersecurity strategy and how they lead to a holistic approach to the response to cybersecurity threats • Identify and describe recent developments in the privacy area, and how it is related to and can be protected by proactive cybersecurity operations • Identify and describe emerging technologies in the cybersecurity field and their applications				

	• Recognise the principles of Safer Internet awareness and how cyber awareness becomes a critical factor of vulnerability for cybersecurity on individual or organizational level. • Define and describe the various professional certifications that are available in the area of cybersecurity and network and information security, and how they are applicable to different parts of a comprehensive cybersecurity architecture and related operations		
Prerequisites	None	Co-requisites	CYB600
Course Content	Introduction: The pace of current developments in cybersecurity and the way that they can influence cybersecurity architecture and operations in organizations and governments. Statistics and major cyber attacks / incidents in recent years. Law and Policy: Recent developments in law and policies at the national, European and international level. How these developments can impact the way that cybersecurity operations are conducted. Rising importance of privacy and associated policies. Implications of the expanding usage of cloud services. Strategy: National (including Cyprus) and European cybersecurity strategies, how they fit together, national and international cooperation, common and special threats, differences between national and organizational strategies, connections to the areas of cybercrime, cyberdefence and related external affairs. Critical Information Infrastructure Protection. Cybersecurity as a factor of growth and the Cybersecurity Ecosystem: The importance of cybersecurity for businesses and organizations in general and the interrelations with the other policies. How cybersecurity is a factor of growth and economic development of a business or a whole country. The Cyberecurity ecosystem is in constant evolution and a professional needs to make sure keeping up with it. As cybersecurity as a field has grown in scope and influence, it has effectively become an ‘ecosystem’ of multiple players, all of whom either participate in or influence the way the field develops and/or operates. It is crucial for those players to collaborate and work together to enhance the security posture of communities, nations and the globe, and security consultants have an important role to play in facilitating this goal, in order to achieve a collaborative security in cyberspace. Emerging technologies: Emerging technologies, both in the cybersecurity and in other technological domains, implications on current cybersecurity practices, penetration of technologies that are		

	vulnerable to cyber attacks in all aspects of daily life, implications on vital societal functions. Safer Internet: national, European and international efforts in the Safer Internet area, importance of cyber awareness raising for both of these areas, importance and effects of a high level of cyber safety awareness on individual or organizational level, links and effects to other cybersecurity awareness raising initiatives, Better Internet for children as a key for an innovating society. Professional Certifications: Introduction to the different information security and cybersecurity professional certifications that are available, importance of their combination with academic qualifications, areas of specialization, additional cybersecurity areas covered. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the latest developments in the cybersecurity area and their related implications.
Teaching Methodology	Face – to – face
Bibliography	National, European and international cybersecurity strategy, policy and legal documents IEEE Journals, Magazines and Websites (ISC)^2 Journals, Magazines and Websites ISACA Journals, Magazines and Websites Other professional certification information sources
Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

<table>
<tr><td>Course Title</td><td colspan="5">Master Thesis</td></tr>
<tr><td>Course Code</td><td colspan="5">CYB670</td></tr>
<tr><td>Course Type</td><td colspan="5">Compulsory (for students choosing the Master Thesis)
Optional (for students choosing the elective courses)</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year/3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">Programme coordinator</td></tr>
<tr><td>ECTS</td><td>30</td><td>Lectures/week</td><td>None</td><td>Laboratories/ week</td><td>None</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The course’s purpose is to provide guidance on how to write a successful Master’s Thesis. It aims to provide skills in research methods in the subdiscipline of Cybersecurity. Students will be able to demonstrate the ability to identify and formulate issues critically, independently and creatively as well as to plan and use appropriate methods, undertake advanced tasks within predetermined timeframes, and to contribute to the formation of knowledge in the field. Other skills will be related to participation in research and development work in the field of Cybersecurity, which is considered the main part of the thesis. The course also aims to equip the student with the tools required to manage a project as large as a Master’s Thesis, through providing project management techniques. The Master's Thesis course includes research methods stages of reviewing related work, extending existing or developing new ideas, software implementation and testing, analysis and evaluation, and finally writing a Master's Thesis. Finally, it aims to prepare the student for independent work as a recipient of a Master’s degree.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Understand the basic concepts of probability, random variables, statistical inference, hypothesis testing and regression.
• Be aware of their responsibilities as research students, including scientific ethics, and data and code management requirements.
• Communicate research results, including building a scientific argument orally and in writing in the subdiscipline of Cybersecurity.
• Data exploration and statistical analysis of data with the use of statistical tools and probability calculations.
• Select and justify a research topic and use various resources to carry out a literature search and review in the subdiscipline of Cybersecurity.
• Design, execute, interpret and report results from empirical research projects in the subdiscipline of Cybersecurity.</td></tr>
</table>

	• Manage a project in the subdiscipline of Cybersecurity and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources. • Identify real-world problems in the subdiscipline of Cybersecurity to which academic concepts and methods can be realistically applied to improve or resolve the problem situation. • Select and use effectively the methods and techniques appropriate for particular cases in the subdiscipline of Cybersecurity, and plan and manage their work. • Critically evaluate their research project and the proposed solution, as well as recognize and describe legal, social or ethical obligations stemming from the project.		
Prerequisites	The student needs to have completed all core courses of the programme.	Co-requisites	None
Course Content	Part A: Research Methods: The nature of research: Definitions and types of research; research process; topic selection and scope; feasibility and value. Ethics and responsible research. The literature search: Sources of information; differentiating between types of sources; primary, secondary and tertiary sources; using the library and digital databases to conduct efficient literature reviews; searching the Internet; role of the supervisor. Project management: Methods, techniques and tools for research design, and data collection in the subdiscipline of Cybersecurity. Analysis and synthesis: Statistical and qualitative techniques for data analysis; use of appropriate software. Reliability and validity of research projects. Presentation of research findings: Project structure; conventions on citation and quotations; style of writing a research report in the subdiscipline of Cybersecurity. Part B: Thesis: The student selects a topic in the subdiscipline of Cybersecurity from the M.Sc. Thesis topics catalogue which is provided to them by the course's instructor and is consolidated from the previous semester, so that when the semester begins the student starts right away to have enough time to complete it. Once the students receive the topics, they have a deadline to choose a topic. Topics are assigned, given that the students have passed all the pre-requisite courses for a specific topic. At this point, the Department of Computer Science and Engineering mandates that the academic supervisor and student agree upon the topic as well as the expected output from the M.Sc. Thesis, with specific milestones and deliverables. Once a topic is selected and agreed upon with the academic supervisor, the course follows the weekly breakdown structure as that is provided in the Master Thesis Guide. If		

	the topic is jointly set with the industry, then when the student progresses and reaches the field study/development phase, a second (industrial) supervisor is appointed. However, the main supervisory role lies to the academic supervisor. The specific deliverables for each individual student's project must be discussed and decided upon in consultation with the student's supervisor/s. The written thesis is defended orally during a public defense. An Evaluation Committee including the supervisor/s and one external examiner from another university with an expertise on the thesis topic assess the written thesis.
Teaching Methodology	For Part A: Research Methods there will be distance learning research lectures and seminars, as well as a number of distance learning sessions with the instructor. For Part B: Face-to-face and/or online meetings with the supervisor/s.
Bibliography	Any material suitable for the subdiscipline in which the student is undertaking the thesis will be specified by the instructor/s. Howard, K. & Sharp, J.A. (2019). The Management of a Student Research Project, Gower. J. Zobel. (2014). Writing for Computer Science, Springer. W. Navidi (2019). Statistics for Engineers and Scientists, McGraw-Hill Science/Engineering/Math; Latest Edition. Statistical Methods for Engineers (2010). Geoffrey Vining and Scott M. Kowalski, Thomson, Brooks/Cole, Latest Edition. Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Cambridge, MA: Syngress. Argyrous, G. (2011). Statistics for Research: with a guide to SPSS. Los Angeles, CA: Sage. King, R. S. (2012). Research Methods for Information Systems, Dallas, TX: Mercury Learning & Information
Assessment	Written Thesis: 80% Oral Presentation: 20% Assessment Strategy: Each project must involve deliverables falling into the following general categories:

<table>
<tr><td></td><td>
(a) A proposed solution to a real-world problem in the subdiscipline of Cybersecurity.
(b) A proof of concept, which demonstrates the validity of the proposed solution.
(c) Clear indication of knowledge of relevant work by others in the subdiscipline of Cybersecurity.
(d) The selection and application of appropriate theoretical concepts and methods.
(e) A project thesis of between 12,000 to 16,000 words.

Projects will be marked in two ways.
Firstly, according to the following scheme:
<table>
<tr><td>1. Project justification including its relationship to the current state of the art in Cybersecurity</td><td>10%</td><td>20 marks</td></tr>
<tr><td>2. Ability to select and use appropriate methods and techniques</td><td>10%</td><td>20 marks</td></tr>
<tr><td>3. The clarity, coherence and succinctness with which the solution is developed</td><td>20%</td><td>40 marks</td></tr>
<tr><td>4. Novelty. Does the work improve significantly the current state of the art in Cybersecurity?</td><td>20%</td><td>40 marks</td></tr>
<tr><td>5. Ability to critically review the project and assess its implications for future work in Cybersecurity in view of the project recommendations and conclusions</td><td>10%</td><td>20 marks</td></tr>
<tr><td>6. Project Management: Ability to plan and control the project</td><td>10%</td><td>20 marks</td></tr>
<tr><td>7. Oral presentation :</td><td>20%</td><td>40 marks</td></tr>
<tr><td>Total</td><td>100%</td><td>200 marks</td></tr>
</table>

In addition, students are reminded about presentation issues:
• Is the document/project format (including spelling) of good quality?
• Is it well organized into appropriate sections?
• Is the style of language used appropriate for an academic report?
</td></tr>
<tr><td>Language</td><td>English</td></tr>
</table>

<table>
<tr><td>Course Title</td><td colspan="5">Research Methods in Cybersecurity</td></tr>
<tr><td>Course Code</td><td colspan="5">CYB635</td></tr>
<tr><td>Course Type</td><td colspan="5">Optional (for students choosing the elective courses)</td></tr>
<tr><td>Level</td><td colspan="5">Master (2nd Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">2nd Year / 3rd Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">TBA</td></tr>
<tr><td>ECTS</td><td>10</td><td>Lectures / week</td><td>none</td><td>Laboratories / week</td><td>none</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">The student acquires the necessary skills to enable the successful completion of scientific experiments and their analysis. Established research methods for independent research are introduced using methodical processes.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Explain the scientific method
• Discuss the various types of research
• Assess data through descriptive statistics
• Create correct scientific experiments
• Propose critical analyses of data based on statistical tests
• Explain correlation and regression evidence as part of the analysis of an experimental result</td></tr>
<tr><td>Prerequisites</td><td colspan="2">None</td><td>Co-requisites</td><td colspan="2">CYB600</td></tr>
<tr><td>Course Content</td><td colspan="5">The nature of research:
Definitions and types of research; research process; types of research methods; feasibility and value; Statistical and qualitative techniques for data analysis; use of appropriate software
Descriptive Statistics:
Frequency Distributions; Proportions and Percentages; Nominal, Ordinal and Interval Data;
Cumulative Distributions; Cross-Tabulations; Mode, Median, and Mean; Range, Variance and Standard Deviation; Graphical Representations
Probability and the Normal Curve:
Probability; Probability Distributions; Characteristics of the Normal Curve; Random Sampling; Sampling Error; Sampling Distribution of Means; Standard Error; Confidence Intervals; The t Distribution; Proportions; Generalizing From Samples to Populations</td></tr>
</table>

	Decision Making The Null Hypothesis; The Research Hypothesis; Levels of Significance; Standard Error; Two Sample Tests of Proportions; Analysis of Variance; The Sum of Squares; The F Ratio; Nonparametric Tests; The Chi-Square Test; The Median Test Association Methods Correlation; Strength and Direction of Correlation; Curvilinear Correlation; Correlation Coefficient; Pearson's Correlation Coefficient; The Regression Model; Regression and Pearson's Correlation; Spearman's Rank-Order Correlation Coefficient; Goodman's and Kruskal's Gamma; stration: Goodman's and Kruskal's Gamma. Program-specific content As this course is taught in a variety of Master's programs offered by the department of Computer Science, the last part of the course will discuss specific research methods for each discipline. The specific topics will be provided by the instructor of the course according to the specific needs of the audience.
Teaching Methodology	Face – to – face
Bibliography	Edgar, T. W. and Manz, D. O. Research Methods for Cyber Security. Cambridge, MA: Syngress. Argyrous, G. Statistics for Research: with a guide to SPSS. Los Angeles, CA: Sage. King, R. S. Research Methods for Information Systems, Dallas, TX: Mercury Learning & Information Cohen, P. R. Empirical Methods for Artificial Intelligence, Cambridge, MA: The MIT Press.
Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	CYB615				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Dr Ioanna Danidou				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course provides an overview of the broad and constantly emerging field of cybersecurity policy, governance, law and compliance. The importance of the role of security policy is discussed.				
Learning Outcomes	Upon succesful completion of this course, students should be able to: • State and identify concepts relating to organizational cybersecurity policy, governance mechanisms, applicable legislation and compliance requirements for information security. • State and interpret the different components of a comprehensive organizational cybersecurity policy. • State and interpret the role of security policy within an organization and its position with relation to other controls within a comprehensive cybersecurity environment. • Describe the role of corporate governance with regards to cybersecurity, and the business reasons for implementing a cybersecurity function. • Recognize and explain major applicable legislation and regulatory framework (local, European, international). • Define, explain and exemplify compliance requirements in relation to cybersecurity, information security, data protection (privacy, anonymity) and critical information infrastructure protection.				
Prerequisites	None	Co-requisites	CYB600		

Course Content	Introduction: Concepts of cybersecurity, its relationship with network and information security, cybercrime, cyberdefence, and related definitions. Concepts of policy, governance, related law and compliance, and the relationships between them. Principles: Information security components and concepts, confidentiality, integrity, availability. Policy: definition, role of policy in an organization, statement of management purpose and organizational objectives, description of organizational approach, standards, baselines, guidelines, procedures. Governance: Role of cybersecurity and information security in the organization, levels of responsibility, the different personnel roles: information owner, information custodian, administrator, solution provider, change control, human resources, user. Certification and accreditation. Law: Relevant laws and legal/regulatory frameworks on the national, European and international level. Different types of law related to cyberattacks – computer as the means, computer as a victim. Problems of jurisdiction, borderless nature of cybercrime, relevance and importance of data protection and privacy, investigations. IT and Law: Introduction, Terminology, and the Nature of Cyberspace and Threats. Cyber-regulation and cyber-regulatory theory. Cyberproperty and Intellectual Property. Cyber-rights, Speech Harm, Crime and Control. Roles of International Law, the State, and the Private Sector in Cyberspace. Authentication and Identity Management. Speech, Privacy and Anonymity in Cyberspace. Trust. Compliance: Reasons for specific cybersecurity legislation beyond cybercrime, compliance requirements, self-assessment, auditing principles, audit process. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on reasons behind and expected benefits of compliance requirements and on recent/future developments.
Teaching Methodology	Face – to – face
Bibliography	*“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *“Information Security Governance: A Practical Development and Implementation Approach”*, by Krag Brotby

	“Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats”, by Scott E. Donaldson *“Cyber Security and IT Infrastructure Protection”*, by John R. Vacca *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

Course Title	Cybersecurity Risk Analysis and Management				
Course Code	CYB645				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Dr Nicos Tsalis				
ECTS	10	Lectures / week	3 hours/14 weeks	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental concepts of cybersecurity risk analysis and management, as well as its position as the foundation for cybersecurity protective mechanisms. It covers a wide range of principles and processes related to risk management and sets the scene for the development of comprehensive cybersecurity controls to protect an organizations assets according to the risk appetite of senior management.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the underlying principles of risk analysis and management and the purpose and benefits behind such activities • Explain the terms used, such as risk, analysis, management, vulnerability, threats, actors, impact, risk matrix, etc. • Recognise the difference between vulnerabilities and threats. • Classify and describe a number of different risk assessment/management methodologies. • Classify and describe different assets and their values (including tangible and intangible assets). • Identify and explain various threat sources and the impacts that their materialization may manifest. • Describe the risk management process, as it pertains to the protection of assets. • Evaluate and select appropriate risk treatment options according to the combination of impacts and probabilities that the risk analysis has produced.				
Prerequisites	None	Co-requisites	CYB600		

Course Content	<u>Introduction:</u> Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme. <u>Principles:</u> Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. <u>Assets:</u> Tangible and intangible assets in the cyber world (hardware / software / data, classification, criticality based on the importance and value to organization (not just monetary), dependencies, potential for critical national infrastructure. <u>Vulnerabilities:</u> Sources of cyber vulnerability, complexity of modern software, attack surface of modern systems, development of software for functionality and not with security considerations, existing known and zero-day system vulnerabilities, vulnerability databases and open information. <u>Threats:</u> Cyber threat categorization, sources, motivation, type, technical vs. non technical (e.g. attacks to cooling systems to disrupt cyber systems), threat actors, exploitation of cyber vulnerabilities leading to impact and associated likelihood. <u>Risk analysis:</u> Risk as a combination of possible impact of a threat exploiting a vulnerability and the probability of such an impact occurring, evaluation of cyber risks, categorization, qualitative and quantitative risk analysis, pre-requisites for meaningful quantitative cyber risk assessment, methodologies, risk register. <u>Risk management:</u> Risk evaluation and associated selection of risk treatment options, effects and selection of risk avoidance, mitigation, transfer, acceptance (or a combination thereof), risk management as an iterative process, risk profile stemming from modifications in an organisation's environment, building an organisation's cybersecurity control environment from the results of risk analysis, introduction to basic cybersecurity controls. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical uses challenges of risk analysis and management in real environments.
Teaching Methodology	Face – to – face
Bibliography	*"Effective Cybersecurity: A Guide to Using Best Practices and Standards 1st Edition, by Willian Stallings* *"Cyber-Risk Management" by Atle Refsdal, Bjørnar Solhaug, Ketil Stølen*

	Samimi, A., 2020. Risk Management in Information Technology. Progress in Chemical and Biochemical Research, pp.130-134. *“Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”*, by Evan Wheeler *Tarek, M., Mohamed, E.K., Hussain, M.M. and Basuony, M.A., 2017. The implication of information technology on the audit profession in developing country. International Journal of Accounting & Information Management.* *“How to Measure Anything in Cybersecurity Risk”*, by Douglas W. Hubbard and Richard Seiersen *“The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit)”*, by Anne Kohnke and Dan Shoemaker
Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

Course Title	Incident Response and Forensic Analysis				
Course Code	CYB655				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Dr Dimitrios Baltzatzis				
ECTS	10	Lectures / week	1 hours/14 weeks	Laboratories / week	2 hours/14 weeks
Course Purpose and Objectives	The objective of this course is to introduce concepts and techniques related to the topics of incident response and forensic analysis. The course prepares students to address the nature and scope of cyber incident handling, damage control, service continuity, forensic analysis, service/data restoration, and incident reporting. Students will also focus on learning: • how to properly investigate incidents and design, develop, and deploy incident response plans. • how to properly conduct a digital forensic investigation.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Understand Incident Response and manage Cyber Incidents, identify different kinds of attacks methods to counter their effects • Incident Handling and Response Methodologies • Review the fundamentals of incident response and learn how to build an IR team and effective playbook for handling incidents. • Describe how CSIRT is managed and staffed. • Define and describe the main phases of incident response phases, preparation, identification, containment, eradication, recovery, follow-up, contact an incident respond analysis. • Create an Incident Response Plan • Prepare a Disaster Recovery Plan • Where and how to track the incident • Scoping, defining, and communicating about the incident. • Collect evident data from the incident. • The fundamentals of digital forensics, • Identify and evaluate key forensic analysis techniques • Forensic Imaging, Analyzing System Storage • Contact a forensic analysis by examine the system memory • Analyze issues regarding evidence collection, • Write an incident and forensics analysis report				

<table>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>CYB600</td></tr>
<tr><td>Course Content</td><td colspan="3">• Introduction to Incident Response
• Incident Response Policy
• Incident Handling
• Incident Recovery
• First responder procedures
• Digital Forensics Investigation Process
• Investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process.
• Hard disks, removable media and file systems,
• Windows forensics, duplication/imaging of forensic data, recovering deleted files and hidden or deleted partitions,
• Steganography and image forensics,
• Memory forensics
• Log analysis, password crackers
• Email tracking,
• Technical forensics tools and techniques (Autopsy, FTK, etc.)</td></tr>
<tr><td>Teaching Methodology</td><td colspan="3">Face – to – Face</td></tr>
<tr><td>Bibliography</td><td colspan="3">“<em>Practical Cyber Forensics</em>”, Niranjan Reddy, Apress, 2019,
“Digital Forensics Basics: A Practical Guide Using Windows OS”, Nihad A. Hassan, Apress 2019
<em>Digital Forensics with Kali Linux,</em> Shiva V. N. Parasram<strong>,</strong> <em>Second Edition, 2020 Packt Publishing</em>
Cybersecurity Incident Response, How to Contain, Eradicate, and Recover from Incidents, Eric C. Thompson
<em>“Incident Response & Computer Forensics, Third Edition”</em> by Jason T. Luttgens and Matthew Pepe
<em>“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”</em>, by Leighton Johnson
<em>“The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics”</em>, by John Sammons
<em>Investigating Windows Systems by Harlan Carvey, 2018 Elsevier</em>
<em>“Digital Forensics with Open Source Tools”</em>, by Cory Altheide and Harlan Carvey
<em>“Digital Forensics Processing and Procedures”</em>, by David Lilburn Watson and Andrew Jones
<em>Digital Forensics and Incident Response, Gerard Johansen, 2020 Packt Publishing</em>
IEEE Journals and Magazines</td></tr>
</table>

<table>
<tr><td>Assessment</td><td><table><tr><td>Class participation and attendance</td><td>10%</td></tr><tr><td>Examinations</td><td>70%</td></tr><tr><td>Assignments</td><td>20%</td></tr><tr><td></td><td>100%</td></tr></table></td></tr>
<tr><td>Language</td><td>English</td></tr>
</table>

Course Title	Cyber Threat Intelligence (CTI)				
Course Code	CYB660				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year/ 1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	1 Hours / 14 weeks	Laboratories / week	2 Hours / 14 weeks
Course Purpose and Objectives	The course will help students: • become familiar with the CTI lifecycle, • understand common intelligence formats, • explain the different types of threat actors and what impact they can have on an organisation. • understand the adversary. • gather intelligence requirements. • formulate a collection plan and align relevant sources and agencies • analyse information in order to produce actionable intelligence. • identify, collect, and integrate intelligence feeds. • understand the intelligence requirements of an organisation.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Find, evaluate, and integrate CTI sources • Identify sources of information about threats to an organization • Produce CTI from public and private data sources • Disseminate threat intelligence and threat findings for decision-makers • Apply CTI models including the Diamond Model, Cyber Kill Chain, F3EAD, the Intelligence Cycle, OODA, MITRE ATT&CK et.al • Identify how threat actors conduct activities in cyberspace to achieve their objectives. • Discover previously unknown threats • Logically assess and criticize threat intelligence from any source and improve your own • Explain how CTI is used within an organisational context				

	• Explain what the intelligence cycle is and how it is used by CTI analysts to produce actionable intelligence • Safely probe, infiltrate and monitor adversary campaigns • Use Structured Analytics Techniques to attribute cyber attacks • Produce threat intelligence products such as reports, briefings and IOCs • Explain how vulnerabilities in information systems are discovered. • Applying cyber intelligence to make recommendations for changes to information system security design, implementation, policies, and practices		
Prerequisites	None	Co-requisites	CYB600
Course Content	• What is CTI, Defining CTI Analysis, • Advantages of CTI • Understanding CTI • Objectives of CTI • Tactical intelligence • Operational intelligence • Strategic intelligence • The Six Phases of the CTI Lifecycle and Frameworks • Analytical Frameworks for CTI • Attack Lifecycle, Kill Chain, Diamond • CTI Environment • Applying Intelligence • Collecting Intelligence • Generating Intelligence • CTI for Security Operations • CTI for Incident Response • CTI for Vulnerability Management • CTI for Vulnerability Management • CTI for Risk Analysis • CTI for for Digital Risk Protection • Clarify your CTI needs and goals • Developing the CTI team • How organizations use CTI • Case studies		
Teaching Methodology	Face – to – Face		
Bibliography	• Cyber Threat Intelligence_ The No-Nonsense Guide for CISOs and Security Managers, Aaron Roberts (2021) • Incident Response with Threat Intelligence, Roberto Martinez (2022) • Practical Threat Intelligence and Data-Driven Threat Hunting, Valentina Palacín (2021)		

	• The Threat Intelligence Handbook Christopher Ahlberg (2019)
Assessment	Class participation and attendance 10% Examinations 70% Assignments 20% 100%
Language	English

Appendix II

“Cybersecurity (18 Months/90 ECTS, Master of Science)”

TABLE 1: STRUCTURE OF THE PROGRAM OF STUDY

DEGREE REQUIREMENTS	**ECTS**
All students pursuing the M.Sc. in Cybersecurity program of study must complete the following requirements:	
Compulsory Courses	60
Master Thesis OR Research Methods course and Two (2) Elective Courses	30
Total Requirements	**90**

DEGREE REQUIREMENTS		**ECTS**
Compulsory courses		**60**
CYB600	Introduction to Cybersecurity	10
CYB605	Communications and Network Security	10
CYB610	Cryptography	10
CYB620	Cybersecurity Architecture and Operations	10
CYB625	Ethical Hacking and Penetration Testing	10
CYB640	Special Cybersecurity Topics	10
Master Thesis OR Research Methods course and Two (2) Elective Courses		**30**
CYB670	Master Thesis OR	**30**
CYB635	Research Methods **and** Two (2) Elective courses from the list below (to select one specialization comprised out of two courses). Specialization courses cannot be given independently.	**10** **20**
Elective courses (only if Master Thesis is not selected)		
Audit and Governance		
CYB615 Cybersecurity Policy, Governance, Law and Compliance		10

CYB645 Cybersecurity Risk Analysis and Management	10
Incident Planning, Response, and Forensics	
CYB655 Incident Response and Forensic Analysis	10
CYB660 Cyber Threat Intelligence	10

European University Cyprus

INTERNAL REGULATION

"PERFORMANCE APPRAISAL OF FACULTY AND SPECIAL TEACHING PERSONNEL"

75th Senate Decision: 7 April 2022

97th Senate Decision: 25th July 2023

The Senate approved the following Internal Regulation which revises and substitutes the existing Charter provisions on 'Internal Regulations on Faculty Ranking and Conditions of Service' (Annex 6, Article 6). The "***Performance Appraisal of Faculty and Special Teaching Personnel***" Internal Regulation supports and facilitates the process of self-improvement of the EUC Faculty and Special Teaching Personnel by focusing on the appraisal and developmental nature of the process. It takes place every two years and is submitted online by all Faculty and Special Teaching Personnel through the University HRIS system.

1. Purpose of Performance Appraisal

The main purpose of the Performance Appraisal process is the professional development of Faculty and Special Teaching Personnel. The Performance Appraisal process aims to support and facilitate Faculty and Special Teaching Personnel self-improvement through helpful and constructive feedback and critical self-assessment. The Internal Regulation enables short and long-term professional planning and development with self-improvement as the ultimate aim. The process aims at a "tailored" self-directed self-improvement through critical reflection and identification of areas of strength and weaknesses; the process further aims to appraise the individual's development, performance and attainment of goals within the scope of the individual's field, areas of expertise and scholarly activities.

With this Internal Regulation, Faculty and Special Teaching Personnel will engage in the process of Performance Appraisal every two years as a positive force towards continued professional development and accomplishment. The appraisal process will record the Faculty's performance in the areas of (i) Teaching, (ii) Research[1], and (iii) Service to the University, Community, and Profession.

[1] For Special Teaching Personnel, research involvement and activity will be considered an additional advantage.

Each Faculty and Special Teaching Personnel will submit a Performance Appraisal every two years (See Appendix: Faculty & Special Teaching Personnel Performance Appraisal Report). Section A of the Performance Appraisal Report will be submitted to the Chairperson of the Department by the announced deadline.

2. Performance Appraisal Categories

2.1 Teaching

Effective teaching at European University Cyprus is a standard that cannot be compromised. It involves mastery of the subject matter, the ability to intellectually stimulate students, and effectiveness in communicating the skills, methods and content of one's discipline and specialization area. It entails a spirit of scholarly involvement necessary in continually revising courses and the undertaking of efforts to sustain a high level of teaching potential and constant improvement of teaching skills. Effective teaching also implies ongoing and constructive engagement with colleagues with the goal of intellectual development and improvement of teaching methodology and material. Furthermore, the constant improvement of coursework and program development is attained by participation in academic professional development training, schemes, programs, seminars, and colloquia organized by the University and/or other educational institutions.

In Section A of the Performance Appraisal Report, the Faculty and Special Teaching Personnel should discuss their accomplishments in courses taught, and activities aimed at sustaining and improving teaching effectiveness. The effort and energy applied in activities, such as course development, course revision, and/or development of new technologies, instructional publications, activities, methodology and/or teaching material to enhance the learning environment should also be noted. Faculty serving in professional programs should outline teaching within their professional service when relevant (e.g., clinical teaching in medicine, dentistry, physiotherapy, nursing, psychology, etc.). Attention also needs to be paid to accessibility and student academic guidance and support, as well as to summaries of student evaluations and feedback reports.

2.1 Research

Research output is a fundamental requirement at European University Cyprus. Research encompasses the pursuit of pertinent questions with the utilization of methodologies and discipline learning, is closely informed by thorough investigation, and aims at academic advancement and the accumulation of new knowledge. Furthermore, research should also serve an academic interest that extends beyond the boundaries of the immediate University community.

Research output can take many forms, such as:

- published research: article(s) in scholarly periodical(s), chapter(s) in scholarly publication(s), book(s), paper(s) presented at professional conference(s);
- contribution in research conference/event organization, seminars and workshops; and/or

- other forms of curatorial and practice-based research (these categories may include among others composition and conducting of music works, performance, digital media, design, and exhibitions).

In Section A of the Performance Appraisal Report, the Faculty (and Special Teaching Personnel on an optional basis) should prepare a statement/list that discusses/presents current research that is completed or still in progress. The Faculty is encouraged to note the degree and kind of support received from the University (e.g., teaching load reduction, time-off, research grant, etc.) that contributed to the successful completion of his/her scholarly endeavors. In this Section, the Faculty could also indicate what they consider as their future needs and how the University may accommodate and/or support them.

2.3 Service to the University, Community and Profession

Service to the University, Community and Profession encompasses a wide range of contributions made by a Faculty member to their academic institution, surrounding community and respective professional field. It may involve active engagement in activities that benefit various areas that would count as instances of professional development. As educators, Faculty need to pursue professional development in activities that improve instructional and research capabilities, qualifications, etc. The quality of contributions, not merely the numbers of committees and assignments, remains a significant consideration. The University also values contributions to planning, governance, and leadership in achieving the goals of the University, working with students outside the classroom and, wherever appropriate, making the University resources accessible to the wider community.

In Section A of the Performance Appraisal Report, the Faculty and Special Teaching Personnel should prepare a statement that discusses contributions made to the University and the local and wider community in the area of service. Activities such as committee memberships and offices held; providing mentorship and guidance to students, professionals, or society; collaborating with community organizations; participating in outreach programs, and actively contributing to professional and academic associations, committees pertaining to higher education formed and appointed by the government; contribution to event organization; training activity; reviews of manuscripts submitted for publication to university presses or scholarly journals; grant proposals/applications submitted to government agencies or learned and professional societies; review of grant applications submitted to government agencies or learned and professional societies; participation in education/training programs and pursuing of additional qualification/degrees; outreach activities, classroom work, and/or work with students outside the classroom should be outlined. Activities demonstrating involvement in community service and commitment to social responsibility, such as membership in community organizations and volunteer work should be noted. Also, other activities that extend the resources of the University to the wider community should be presented.

3. Performance Appraisal Process

3.1 The Performance Appraisal process will be based on the Appraisal Categories stated above, which are informed by the University's mission, purpose, strategy and objectives.

3.2 A Performance Appraisal Review Committee will be set up every second year by each Department. The Performance Appraisal Review Committee will consist of three members:

1. The Chairperson of the Department. In case the Department Chairperson does not hold the rank of Professor or Associate Professor, s/he will be replaced by another Professor of the Department following elections by the body of Professors of the Department. In Departments where there is no Faculty at the rank of Professor, the Chairperson will be replaced by an Associate Professor following elections by the body of Associate Professors of the Department. In Departments where there is no Faculty at the rank of Professor or Associate Professor, the Chairperson will be replaced by a Professor from another Department of the same School whose field of specialization is as close as possible to the Department's specialization. In this case, the assignment of the Committee member will be made by the Dean of the School and will be effective for a two-year term.
2. Two Professors of the Department elected by the body of Professors of the Department for a two-year term; in case the Department has no adequate Faculty at the rank of Professor, the members of the Committee will be elected from the body of Associate Professors of the Department. In case the Department has no adequate Faculty at the rank of Professor or Associate Professor the rest of the Committee members will be selected from the Professors of the other Departments of the same School whose field of specialization will be as close as possible to the Department's specialization. In this case, the assignment of the Committee member(s) will be made by the Dean of the School and will be effective for a two-year term.

3.3 The Performance Appraisal Review Committee should elect the Chair in its first meeting.

3.4 In case the appraisee is a member of the Performance Appraisal Review Committee, he/she cannot participate in the process. In this case (and only in this case) the Performance Appraisal Review Committee becomes a two-member committee.

3.5 The Performance Appraisal Review Committee is in charge of conveying the expectations of the Performance Appraisal process to Faculty and Special Teaching Personnel.

3.6 Section A of the Performance Appraisal Report document (See Appendix: Faculty & Special Teaching Personnel Performance Appraisal Report) will be used for recording an individual's performance, which will be completed and signed by each Faculty and Special Teaching Personnel and submitted to the Performance Appraisal Review Committee via the Chairperson of the Department by the announced deadline every second year. The Chair of the Department witnesses through signature the validity of the content of the Performance Appraisal Reports-Section A submitted by the Faculty and Special Teaching Personnel and subsequently forwards it to the Chair of the Performance Appraisal Review Committee for the initialization of the appraisal process.

3.7 The Performance Appraisal Review Committee will carry out jointly the appraisal review of each Faculty member and Special Teaching Personnel member every two years.

3.8 The Performance Appraisal Review Committee will review the Performance Appraisal Report-Section A, give instructions for clarification/remedy in cases of ambiguity, verify the outcome of the appraisal of each Faculty and Special Teaching Personnel, and provide recommendations.

3.9 The Performance Appraisal Review Committee jointly will meet with each Faculty and Special Teaching Personnel to discuss the outcome of the review process and their recommendations before the end of the academic year. The Performance Appraisal Review Committee and the involved Faculty or Special Teaching Personnel should jointly fill in and sign the Performance Appraisal Report-Section B at the time of their meeting. The Faculty/Special Teaching Personnel may add her/his own comments.

3.10 The Performance Appraisal Report-Section B, based on the above stated Performance Appraisal Categories, will take the form of supportive and constructive feedback with specific agreed goals to be reached by the end of the following Performance Appraisal period.

3.11 Upon completion of the appraisal process, the final documents reach the School Administration Office, the Chairperson of the Department, the Dean of the School, the Vice Rector of Academic Affairs, and the Director of Human Resources before the end of the academic year.

3.12 The Committee also submits via its Chair to the Department Council a report on the overall professional development needs of the Department to be presented and discussed at the respective Department Council.

APPENDIX

FACULTY & SPECIAL TEACHING PERSONNEL
PERFORMANCE APPRAISAL REPORT

SECTION A:

(To be completed by the Faculty/Special Teaching Personnel member)

NAME:

DEPARTMENT:

SCHOOL:

ACADEMIC YEARS:

Please record your activities of your individual performance relating to each of the following categories during the last two academic years. In doing so, please refer to the activities/actions described in the Internal Regulation of the "Performance Appraisal of Faculty and Special Teaching Personnel".

1. TEACHING

A) **Courses, Student Academic Advising, Support and Accessibility, and Supervision** (provide a list of courses taught, thesis and dissertations supervised, and briefly describe the provisions made to enhance the accessibility of your courses, your academic advising, etc.)

B) **Quality & Effectiveness** (briefly describe your teaching methodology, explaining in particular the effort undertaken for quality, innovation, and effectiveness. If relevant, provide information on course design, documentation, development and revisions, instructional publications, material production, teaching resources, program development and revisions, instructional innovation, appropriateness of assessment, etc.)

C) Willingness, Cooperation and Flexibility

D) Other

2. RESEARCH

A) Refereed Journal Publications (authors, year, article title, journal tile, volume, issue, pages; in the language of the publication).

B) Refereed Book Publications (authors, year, book title, city; publisher; in the language of the publication).

C) Refereed Book Chapter Publications (authors, year, chapter title, book title, pages; in the language of the publication).

D) Funded Research Projects (duration of project, title, funding body, total funding of project, role in the project*).

*Project Role: i.e. Principal Investigator, Scientific/Project Coordinator, Research Team Member, Researcher, Assistant Researcher, etc.

E) Other Refereed Research Activities** (including in the categories of curatorial and practice-based research, such as composition, conducting of music works, performance, digital media, design, and exhibitions)

**do not include conferences and dissemination activities

3. SERVICE TO THE UNIVERSITY, COMMUNITY AND PROFESSION

A) **Service to the University** (e.g. program coordination, administration responsibilities, committee memberships, event organization, etc., at the program, Department, School and University level)

B) **Service to the Community** (e.g. committee memberships, event organization, etc. outside the University -locally and internationally)

C) Service to the Profession and Self-Development (e.g. review activities, professional development activities, etc.)

D) Other Service (e.g. funded activities or work, consultancy projects)

Date of Submission:...

____

Signature of the Faculty/Special Teaching Personnel member

____

Signature of the Chairperson of the Department confirming the validity of the content of the Performance Appraisal Report

Date:...

<u>SECTION B:</u>

(To be jointly completed and signed by the Performance Appraisal Review Committee and the Faculty/Special Teaching Personnel member)

NAME:

DEPARTMENT:

SCHOOL:

ACADEMIC YEARS:

Please jointly fill in and sign at the time of your meeting with the involved Faculty member/Special Teaching Personnel Section B of the Appraisal Report. The Performance Appraisal Review Committee provides its recommendations and the involved Faculty/Special Teaching Personnel member may add comments in the last section of the Report.

The Report is based on the Appraisal Categories described in the Internal Regulation of the "Performance Appraisal of Faculty and Special Teaching Personnel" and aims to provide supportive and constructive feedback with specific agreed goals to be reached by the end of the following Performance Appraisal period.

1. TEACHING

Overall Appraisal of Teaching:

Agreed goals to be reached by the end of the two-year Performance Appraisal period:

2. RESEARCH

Overall Appraisal of Research:

Agreed goals to be reached by the end of the two-year Performance Appraisal period:

3. SERVICE TO THE UNIVERSITY, COMMUNITY AND PROFESSION

Overall Appraisal of Service to the University, Community and Profession:

Agreed goals to be reached by the end of the two-year Performance Appraisal period:

Comments for Overall Performance Appraisal:

By the Performance Appraisal Review Committee:

By the Faculty/Special Teaching Personnel member
(Comments may include suggestions on how the Department/School/University may support her/him to improve her/his performance by the end of the Performance Appraisal period):

Comments by Review Committee Member:

Date of Meeting: ....

____
Signature of the Chair of the Performance Appraisal Review Committee

__________________________ __________________________
Signature of Members of the Performance Appraisal Review Committee

____
Signature of the Faculty/Special Teaching Personnel member

Appendix IV

European University Cyprus

INTERNAL REGULATION:

EUC FRAMEWORK ON MENTORING SCHEME FOR NEWLY HIRED FULL-TIME ACADEMIC STAFF AND/OR PART-TIME ACADEMIC STAFF

89th Senate Decision: 7 April 2022

EUC Framework on Mentoring Scheme for Newly Hired Full-Time Academic Staff and/or Part-Time Academic Staff

Basic Premises of Mentoring:

A Mentoring program is based upon providing a support system to promote a symbiotic interchange and it embraces the primary pillars of the mentor concept:
Manages the relationship
Encourages
Nurtures
Teaches
Offers mutual respect
Responds to the Mentee's needs

Mentoring is based on promoting a synergetic purposeful conversation and reflection on experience with aim to:

1. Challenge
2. Motivate, and
3. Inspire.

The effectiveness of the process is based on mutual trust, a genuine belief in the process, helping the mentee's ideas to flourish, and inspiration of a vision.

The principles applied include:

Synergy:

- Enriching for both mentor & mentee;
- It's all about learning – not teaching;
- Mentee is empowered to take responsibility of their life.

Relationship:

- Mentoring is a "power-free" partnership;
- Develop mentee's independent thinking –not make them independent.

Uniqueness:

- This is not coaching or counselling;
- Provides direction to channel efforts;
- Nourishes ideas.

Mentoring Schemes

1. Introduction/Induction/On-Boarding/Orientation Program

Basic Premises:

- Aims to familiarize newly hired academic staff (both full-time and part-time) with the educational model of the School and the Department, the basic principles and means of teaching, as well as the rules and policies of European University Cyprus.
- The School/Department introduces its programs' curriculum, the facilities and other necessary information for the newly hired academic staff to integrate effectively and quickly into the programs of study.
- As we have professionals, we began to include support information for their integration into the Cyprus professional community.
- On-boarding is offered when instructors first start. In addition, many instructors who have participated in on-boarding programs are recruited to help with the orientation of new part- or full-time staff. The process of "see one, do one, teach one", further supports their understanding, but more importantly encourages engagement and investment into the program.

2. Dyad Mentoring

Structure Meetings around the Survey on "Students Feedback on their Learning Experience" (SFLE)

- Novice newly hired academic staff can actively be mentored by a senior member of the faculty or leader/line manager.
- Upon receipt of students' feedback/evaluations/surveys, a one-on-one meeting is scheduled to discuss the outcomes.
- While the meeting is designed around the students' feedback, it provides the opportunity for a mentor-mentee discussion that includes not only teaching, but also research, professional development and personal dilemmas, and/or goals.
- By planning the meeting aims to discuss teaching, research, development and personal dilemmas, and goals based on review of students' feedback outcomes, the new members are able to reflect on their personal development. The aim is not only to improve their teaching skills under close supervision, but to help the member become more engaged and invested, and ultimately satisfied.
- At the end of this programmed meeting, a form is co-signed that outlines the items discussed for teaching, research, professional development, etc., including:
    1. Observations/outcomes from students' feedback
    2. Goal-development

3. Goal-activity alignment.
4. Goal-time alignment.

3. Peer-Mentoring Model

- Peer-groups form a critical basis of peer-mentoring. Peer-groups offer:
  1. Psychosocial support: friendship, confirmation, emotional support, empathy;
  2. Mutual professional development;
  3. Collaborative problem solving.
- Schools/Departments can support peer or near-peer mentoring by introducing new members into the networks of the School/Department. This is typically done, by putting new members into committees of the School or Department. Members can be rotated among different committees, until they find a network niche that they feel comfortable in (this part will take careful monitoring by the leadership of the Department/School.)
- Hence, the School/Department encourages peer mentoring by the construction of ad-hoc committees:
  1. This creates deliberate networks – giving a “jump-start” to individual networking;
  2. This creates common goals among the committee/network members;
  3. This ensures peer or near-peer mentoring by frequent meetings imposed by their roles in the committee.
- Finally, by participation in these committees, the newly hired academic staff is introduced and exposed to the other aspects of their duties.

Portfolios

- An electronic portfolio system may include CV material, publications prizes, etc., but reflection and professional development outline as discussed with mentor and advisors.
- Mentoring is a crucial component for portfolio learning, as they assist not only in successfully compiling the information that goes in the portfolio, but also understanding outcomes and devising goals.
- A portfolio is a “living document” that includes both CV – type material, as well as reflection upon goals, key experiences, etc.
- The typical CV update material, included in a Portfolio are:

Contact Information

Biographic Information

Goals

- Educational goals
- Professional goals
- Personal goals

Professional Development

- Educational history
- Certifications
- Memberships
- Awards/recognitions
- Leadership

Achievements

According to year & discipline
e.g. End of placement report and feedback

Academic Courses

- Courses taken by semester
- End of semester report and feedback

Service

Professional service
Community service
Employer service

Conference Attendance

In-Service Professional Development

Scholarly Activity

- Presentations
- Publications
- Research

Curriculum Vitae

- The second section is designed as “reflective portfolio”, to support learning, personal growth and achievement.
- The aim is to be widely used in the assessment of professional learning, as it promotes individuals to review their outcomes and reflect.

Portfolios as a Mentoring Model

- Self-Assessment of Professional Growth through Reflective Portofolios:
    - This involves establishing a critical reflection and learning plan (self-directed learning plan)
    - The portfolio will provide space for reflective pieces by each individual, to reflect on performance, set goals, etc.
    - By creating a safe and supportive environment for candid reflection, this will facilitate structured meetings with a mentor/leader, for feedback on experiences and goals by senior mentors.
    - This will also provide the opportunity to discuss development and design of strategic prompts, so that the individual can move forward in their career path.
    - Portfolios are also effective in promoting leadership development.
- Mentoring Portfolios

- Mentoring enhances the feedback process and stimulates reflection by individuals
- During individual meetings based on the portfolio, mentors, as well as mentees are stimulated by input to introduce subjects for discussion
- Individual meetings begin with highlight the main themes of the previous meeting, and formulating agreements for the upcoming period
- Small group (peer group mentoring) are useful for learning to discuss experiences, developing reflective skills and sharing experiences.

European University Cyprus

Appendix V

SCHOOL	THE SCHOOL OF SCIENCES

COURSE OUTLINE

Course Title	
Introduction to Cybersecurity	
Course / Section	**Semester**
CYS601 N	FALL 2017
Day / Time	**Credits / ECTS**
TU10;TU11;TU12	7
Lecture Room	**Prerequisite(s)**
205	None
Instructor	**Office Telephone Number**
Dr. Yianna Danidou	22559613
Office Room Number	**Office Hours**
125	Monday 11:05 – 12:20 Tuesday 17:00 – 17:50 Wednesday 10:15 – 12:20 14:00 – 15:00
E-Mail	**Website**
y.danidou@external.euc.ac.cy	Moodle.euc.ac.cy
Assessment: (100%)	

Class participation and attendance	10%
Examinations	70%
Assignments	20%
	100%

Course Description:

This course introduces the fundamental concepts and terminology of cybersecurity as a whole, and functions as a short introduction to the large number of cybersecurity topics that are covered within this MSc course.

Learning Outcomes:

Upon succesful completion of this course students should be able to:

- Describe the meaning and position of fundamental cybersecurity concepts and terminology
- Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model
- Classify and describe different cybersecurity components and how they contribute to effective defence
- Classify and describe different potential routes for cyber attacks.

Textbook:

“Introduction to Computer Networks and Cybersecurity”,
by Chwan-Hwa (John) Wu and J. David Irwin

“Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover”, by Lee Mark Zeichner

IEEE Journals, Magazines and Websites

(ISC)^2, ISACA, and other cybersecurity websites

Weekly Breakdown:

WEEK	TOPICS
1	Introduction: Refresh on fundamental networking principles and devices and distributed systems, the context within which cybersecurity (or lack thereof) can be present. Network structure and ways of communication.
2	History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.)
3	History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.)
4	Current importance of cybersecurity, given the connectedness of most of our daily lives. Analysis of critical infrastructures and the position of critical information infrastructures within these – importance of the protection of such systems for the smooth operation of essential services in all areas of life. The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats.
5	Asset protection (including data) as a valuable business operation and its contribution to business survivability.
6	Main principles of cybersecurity – confidentiality, integrity, availability and combinations thereof, resulting in other important cybersecurity concepts and services – accountability, non-repudiation, authenticity, resilience, business continuity and disaster recovery, audit, cybercrime, data / system / network forensics, cyberdefence.
7	Midterm exam
8	Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover.
9	Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover.
10 ***Course/Instructor's Evaluations**	Applicable cybersecurity and IT law Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust.
11 ***Course/Instructor's Evaluations**	Introduction to other courses in this MSc (to aid selection of the elective courses).
12 ***Course/Instructor's Evaluations**	Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc.
13 ***Course/Instructor's Evaluations**	Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.

14 ***Course/Instructor's Evaluations**	**CHRISTMAS HOLIDAYS**
15	**CHRISTMAS HOLIDAYS**
16	**FINAL EXAMINATIONS**
17	**FINAL EXAMINATIONS**

***Please remember to evaluate the course electronically, according to the guidelines that will be sent to you by sms/email.**

Grading system

Letter Grade	Grade meaning	Grade points	Percentage grade
A	Excellent	4.0	90 and above
B+	Very good	3.5	85 – 89
B	Good	3.0	80-84
C+	Above average	2.5	75-79
C	Average	2.0	70-74
F	Failure	0	
I	Incomplete	0	
W	Withdrawal	0	
P	Pass	0	
AU	Audit	0	

Notes:

a) The grade "I" is awarded to a student who has maintained satisfactory performance in a course but was unable to complete a major portion of course work (e.g. term paper or final exam) and the reasons given are acceptable to the instructor. It is the responsibility of the student to bring pertinent information to the instructor to justify the reasons for the missing work and to reach an agreement on the means by which the remaining course requirements will be satisfied. A student is responsible, after consulting with the instructor, for fulfilling the remaining course requirements within the first four weeks of the following semester for which an "I was awarded. In very special cases the instructor may extend the existing incomplete grade to the next semester. Failure of the student to complete work within this specific time-limit will result in an "F" which will be recorded as the final grade.

b) The grade "W" indicates withdrawal from the course before the specified time as explained in the withdrawal policy.

c) Grades of "P" will not be computed into a student's cumulative grade point average but will count towards graduation credits.

d) Grades of "F" will be computed into the student's cumulative grade point average.

e) Students enrolling for an Audit must designate their intent to enrol on an Audit basis at the time of registration. Students registering for a course on an Audit basis receive no credit.

f) Grades for courses taken at another university do not enter into the computation of the cumulative grade point average.

European University Cyprus

Internal Regulations on Academic Ethics and Students' Discipline

1. PREAMBLE

E.U.C. European University - Cyprus is a community of scholars in which the ideals of freedom of inquiry, freedom of thought, freedom of expression, and freedom of the individual are sustained. However, the exercise and preservation of these freedoms and rights require a respect for the rights of all in the community to enjoy them to the same extent. It is clear that in a community of learning, willful disruption of the educational process, destruction of property, and interference with the orderly process of the University or with the rights of other members of the University cannot be tolerated. Students enrolling in the University assume an obligation to conduct themselves in a manner compatible with the University's function as an educational institution. To fulfill its functions of imparting and gaining knowledge, the University retains the power to maintain order within the University and to exclude those who are disruptive of the educational process.

2. POLICY AND PROVISIONS ON ACADEMIC ETHICS

The University has a responsibility to uphold and promote quality scholarship and to ensure that its students understand what academic integrity is. This section outlines the University's policy on dishonest academic performance by its students. Such offences carry penalties. Students should read carefully the Internal Regulations on Academic Ethics and Students' Discipline, and are encouraged to ask Faculty for help and guidance on honest academic practice, particularly in using source material from the Internet. In this way they can avoid any unintentional dishonesty.

2.1. ORIGINALITY

For the purposes of this Policy on Academic Ethics 'original' work is work that is genuinely produced specifically for the particular assessment task by the student whose name is attached to it. Any use of the ideas or scholarship of others is acknowledged. 'Work' includes not only written material but also oral, audio, visual or other material submitted for assessment.

2.2. ACADEMIC DISHONESTY

Academic dishonesty is determined by the extent and the level of intent. In assessing the extent or scale of the dishonesty the instructor will evaluate how much of the work is the student's own after all unacknowledged source material has been removed. In no case can work that is plagiarized be taken into account in determining a grade. Intent to deceive is the single most significant aspect of academic dishonesty. Repeated instances of deception will incur heavy penalties for the student and the violation will be officially and permanently recorded in the student's record.

2.3. PLAGIARISM

Plagiarism is representing the work of somebody else as one's own. It includes the following:

1. submission of another student's work as one's own;
2. paraphrasing or summarizing without acknowledgement of source material;
3. direct quoting or word copying of all or part of a work, ideas, or scholarship of another without identification or acknowledgement or reference;
4. submitting as one's own work purchased, borrowed or stolen research, papers, or projects.

2.4. CHEATING

Cheating is giving or receiving unauthorized help for unfair advantage before, during, or after examinations, tests, presentations or other assessments, such as:

1. collaboration beforehand if it is specifically forbidden by the instructor
2. verbal collaboration during the examination, unless specifically allowed by the instructor;
3. the use of notes, books, or other written aids during the examination, unless specifically allowed by the instructor;

4. the use of electronic devices and mobile telephony to store, transmit or photograph information to or from an external source;
5. the use of codes or signals to communicate with other students in the examination room;
6. looking upon another student's papers and / or allowing another student to look upon one's own papers during the examination period;
7. passing on any examination information to students who have not yet taken the examination;
8. falsifying exam identification by arranging with another student to take an examination in their place or in one's own place;
9. pretending to take the exam but not submitting the paper, and later claiming that the instructor lost it.

2.5. COLLUSION

Collusion is false representation by groups of students who knowingly assist each other in order to achieve an unfair assessment advantage. It involves:

1. representation of the work of several persons as the work of a single student with both parties knowingly involved in the arrangement;
2. representing the work of one student as the work of a group of students with both parties knowingly involved in the arrangement;
3. willing distribution of multiple copies of one's assignments, papers, projects to other students for submission after re-labeling the paper as their own original work.

2.6. FABRICATION

Fabrication is the false representation of research data or 'performance' material as original, authentic work for submission for assessment. Examples are:

1. invention of data;
2. willfully omitting some data to falsely obtain desired results

2.7. PENALTIES AND PROCEDURES

A faculty member, after evaluating the extent of the dishonesty and the level of intent and proving academic dishonesty, may use one or a combination of the following penalties and procedures:

1. requiring rewriting of a paper containing some plagiarized material;
2. lowering of a paper or project grade;
3. giving a failing grade on a paper;
4. lowering a course grade;
5. giving a failing grade in a course;
6. referring the case to the Senate for further action that may include academic suspension or expulsion.

Instructors are expected to report in writing to the Registrar's Office (through their Chairperson of Department) all the penalties they impose, with a brief description of the incident, with copies sent to the Dean of the relevant School and the Rector. Should an instructor announce a failing grade in the course because of academic dishonesty, the student under penalty shall not be permitted to withdraw from the course.

European University Cyprus

Appendix VI

Faculty Professional Development Program 2022-23

A/A		HOURS	DATE ATTENDED
1.	Orientation to European University Cyprus (EUC)	2 hours	28/9/2022
2.	Familiarization with EUC Academic Structures, Processes and Procedures: How to prepare for the Semester	3 hours	28/9/2022
3.	Familiarization with Blackboard Learn Ultra and the Department of Information and Operations Support Structures	2 hours	29/9/2022
4.	Orientation on Research and Mobility at EUC	2 hours	18/10/2022
5.	Artificial Intelligence (AI) in Higher Education	2 hour	20/2/2023
6.	Navigating the Opportunities and Threats of AI Tools in Education	1 hour	14/3/2023
7.	Accessing Blackboard Learn Dashboard	1 hour	21/3/2023
8.	Poll Everywhere	2 hours	24/3/2023
9.	Advance HE “New to Teaching Programme”	25 hours	4th,18th, 25th/5/2023 & 1st, 8th, 15th/6/2023
	TOTAL HOURS ATTENDED	**40 Hours**	

European University Cyprus

APPENDIX VII

Center of Applied and Personal Development (ΚΕ.ΨΥ.Π.Α.)

Aims:

The Center of Applied Psychology and Personal Development (ΚΕ.ΨΥ.Π.Α.) is offering psychological and counselling services to the members of European University Cyprus. The Center was established to promote Prevention, Assessment and Therapy and provide these services to the members of EUC (staff and students) free of charge.

Staff:

The Center is supervised by the School of Humanities, Social and Education Sciences, and the faculty member Dr Panagiotis Parpottas- Assistant Professor and registered Counselling Psychologist, is the Head of the Center. Dr Iliana Dimitriou-registered Counselling Psychologist, is the Specialist Psychologist of the Center who offers psychological services and coordinates all clinical cases. Moreover, a number of postgraduate Clinical and Counselling Psychology students offer psychological services during their supervised Internship. In addition, undergraduate psychology students are given administrative duties in the call center of ΚΕ.ΨΥ.ΠΑ. during their placement. Finally, the Center collaborates with a number of registered Clinical and Counselling Psychologists who supervise the clinical work of the postgraduate Clinical and Counselling psychology students.

Context and Services:

All services are provided to students and staff with discretion and with the strictest confidentiality, as defined by the psychologists' code of ethics and the relevant laws in Cyprus.

As EUC aims to promote the academic and personal development of its students and members of staff, the identification of individuals' needs is of outmost importance and this is achieved by having an 'open door' policy with all members of EUC. Specifically, at the beginning of each semester, all the Schools and administrative departments of the University are informed on the Center's services. In addition, the Center participates in the induction week for newcomer students, informing them on the offered services. During the academic year, there is a continuous collaboration with the schools and administrative departments concerning the referral of students and staff to the Center. Finally, ΚΕ.ΨΥ.Π.Α. liaises with the Speech Language and Hearing Clinic of the University and can offer consultations if necessary to committees such as the Grievance Committee, the Committee of Students with Special Educational Needs (Ε.Φ.Ε.Ε.Α.) and other.

Individuals can receive the Center's services either by contacting directly the call center or by being referred (i.e. use of a referral form in cases of students' referrals by staff). The Center operates only with scheduled appointments and the available services are:

1. Psychological assessment with qualitative methods and quantitative Psychometric tests.
2. Psychotherapeutic interventions for interpersonal difficulties and psychological problems. Therapy sessions are offered in individual and group basis and

normally last up to 12 sessions however after assessment long term therapy may be offered.

3. Risk assessment and crisis intervention.
4. Assessment of students’ psychological difficulties which may impact their academic performance and collaboration with Ε.Φ.Ε.Ε.Α.
5. Referrals to other public or private services for cases of severe psychopathology and other health problems which cannot be talked in the center.
6. Liaison when necessary, with academic and administrative staff for psychological difficulties which may affect the students’ academic and personal fitness.
7. Liaison when necessary, with the department of Human Recourses for psychological difficulties which may negatively impact the academic and administrative staff.
8. Collaboration when necessary, with the University Grievance Committee.
9. Counselling and support to students’ families.
10. Training seminars to EUC staff on psychology topics.
11. Seminars for personal development and prevention of mental health problems.

External Collaborations:

ΚΕ.ΨΥ.Π.Α. has established various external collaborations aiming to enhance it services it offers. The Center or the EUC, are not obliged to cover the cost for therapies provided -when referred- out of the Center to external collaborators such as:

- Registered Clinical, Counselling and Educational Psychologists
- Psychiatrists
- Other medical specialties

Public and private services