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)"-Εξ Αποστάσεως

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

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

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

- **Concentrations (if any):**

  In Greek: Concentrations
  In English: Concentrations

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	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 *CYS645 Cybersecurity Architecture and Operations;* • "Embedded Systems Security" in the course *CYS645 Cybersecurity Architecture and Operations;* and • "Cloud Security" in the course *CYS615 Communications and Network Security.* Moreover, we have updated the course *CYS685 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 for all courses in Appendix I; please see more specifically the courses CYS615 in page 5, CYS645 in page 13, and CY685 in page 43 respectively)	Choose level of compliance:

"Cloud Security" as part of the core curriculum could constitute a 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 *CYS600 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 *CYS675 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 for all courses in Appendix I; please see more specifically the courses CYS600 in page 2 and CYS675 in page 37 respectively).	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 (CYS660)* and one on *Management of Communication and Leadership in High Stress and Crisis Situations (CYS*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 *CSE600 Research methods* and *CYS630 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 *CSE600 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 Thesis 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 *CSE600 Research Methods* we enhanced its independent 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	Choose level of compliance:

	independent research and prepares them for future academic or professional endeavors. Similarly, Indicative examples in the course *CYS630 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 course, 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	We thank the EEC for their comment. As also admitted during the on-site visit, where the same issue 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 activities (which as the EEC validated the lab component is strongly eminent in all practical courses). In the course syllabi the field referring to laboratories was indicated as "None", since this refers to the actual use of physical laboratories, which is not valid in this e-learning programme of study. With the EEC recommendation, we have now revisited all course syllabi and we have	Choose level of compliance:

perhaps the "lab/exercises" component was underestimated, and this merits therefore being clarified and properly documented.	adjusted the teaching methodology wording to refer to the lab hours that are actually allocated in each course. 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 for all courses in Appendix I).	
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 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.	We thank the EEC for this recommendation. As discussed with the EEC, we have extensively considered the recruitment of a high-profile senior faculty member in Cybersecurity both at the programme and the Department, School and Senate level. Hence, in the past and repeatedly, we announced vacancies at either the level of "Associate Professor" or "Professor", as well as at "Any rank" and disseminated the announcement at European and International level. For reasons relating to the paucity of Ph.D. holders in the field, with extended academic background and experience who are not already employed in the industry (which pays much more than any academic position), we did not receive the expected CV with the specific caliber. In our last attempt to do so though (deadline of submission was 1.2.2023; vacancy announced "Any rank"), we are happy to recruit a new faculty at the rank of Assistant Professor (officially starting as of 1.9.2023).	Choose level of compliance:

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 recommendation. 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 responses in items 1.7 and 1.8 in the conventional programme of study).	Choose level of compliance:
1.8 One option could be to concentrate only on the 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	In agreeing with the EEC, we have added two new elective courses in the E-learning programme of study to differentiate it from the conventional. In particular, we have updated the course *CYS685 Incident Response and Forensic Analysis*, and we have added the elective course *CYS660 Cyber Threat Intelligence* and one on *CYS665 Management of Communication and Leadership in High Stress and Crisis*	Choose level of compliance:

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.	*Situations* (please see our response above in item 1.3). In Appendix II you may find the updated programme structure which mirrors these changes.	

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 *CYS655 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. 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	We have taken EEC's comment into serious consideration and we will be calling more 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	Choose level of compliance:

interactions (internationalisation at home).	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 therefore 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 CYS600 Introduction in Cybesecurity. Similarly, we aim to invite guest lecturers from renowned 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 In place of using proctoring tool, it could be considered developing cheating and plagiarism resistant assessment methods. This, in particular for a programme which is followed by working professionals, where the installation of a proctoring tool taking full control over their computers may be found to be unacceptable to their IT departments.	Indeed, it has been observed that the Respondus Lockdown Browser software makes some changes to the user's PC while it is running (i.e. while the student is in the exam) and it might be described as being privacy-invasive. Hence, amongst other reasons, we are currently evaluating another online proctoring solution named "Proctorio", which will provide increased flexibility when setting up the exam and reduce the complexity regarding the way the online proctored exams are being run. We have piloted Proctorio in July's final exams. Proctorio is not a software which makes changes to the user's PC like Respondus, and it does not use or hold any biometrics to authenticate students.	Choose level of compliance:

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. 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	Choose level of compliance:

	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). 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.	Choose level of compliance:
3.5 Introduce School wide mechanisms to assess the quality of research outputs	In accordance with the EEC, members of our Department are implementing a mentoring scheme, where junior faculty are being mentored in grant	Choose level of compliance:

from mentoring to post publication assessment.	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 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, E-Learning students receive continuous academic support in addition to the synchronous teleconferences. The instructor, through the role of the e-moderator and as the facilitator who guides students for effective self-study, employs a range of alternative methods to increase his/her contact time and effectiveness. Consequently, considerable contact time is devoted to students in discussion forums and through emails, through one-to-one teleconferences and group teleconferences aiming at addressing customised needs of individual and group student needs. This model follows the latest pedagogical guidelines and recommendations for the design and development of E-Learning programmes of study distributed by the Cyprus Agency of Quality Assurance and Accreditation in Higher Education (CY.Q.A.A.), including announcements issued by CY.Q.A.A. on 29.4.2020 and 4.5.2020 on E-Learning programmes of study. This model of course faces the 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 working hours and response expected timeframes are presented in the EUC E-Learning Programmes of Study framework (please see Appendix V). This document is intended primarily for all academic staff involved in course design and teaching on the E-Learning programmes of study at European University Cyprus. The document introduces the essential elements of the pedagogical principles and	Choose level of compliance:

	teaching philosophy employed on all E-Learning courses at EUC. The document breaks down these expectations as follows: • academic staff working hours: 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 Blackboard Learn Ultra page of the course. • Student advising support • Administrative support by the Distance Education Unit. All this information is also communicated to students through a Welcome Letter upon enrolment in an E-Learning programme of study (please see Appendix VI), as well on each instructor's course webpage (please see e.g. the interface of the course CYS600 in Appendix VII).	
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 to enhance their e-learning skills, 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 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)	Choose level of compliance:

	scheme. Please find attached the 2022-2023 FPD full programme (Appendix VIII)	
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 senior academic staff in the area of cybersecurity (as explained in item 1.6 above). In addition to our response in 1.6 above on the hiring of a new faculty member to teach Cybersecurity courses, we would like to underline that the conventional programme of study is currently not offered and thus there is not teaching load for staff members. The E-learning programme of study has a manageable number of students and thus currently it does not require additional full-time faculty member to be recruited.	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 Although the current staff of the DLU/TPP and the Content Factory team are providing good services, it is recommended to strengthen the central distance learning unit to offer professional distance/digital education services for students and faculty members, e.g. the Content Factory team could be integrated into the central DLU team, and one or two more instructional designers should be appointed. The services should be bundled in one centre, e.g., a Center for Teaching and Learning.	It is very important both that the Committee positively evaluates the services of the Distance Education Unit, as well as the proposal to enhance its operation and services. European University Cyprus has been offering fully accredited E-Learning Bachelor's (undergraduate) and Master's (postgraduate) programmes of study since 2013. Since then, the Distance Education Unit (DEU) provides the administrative support for the E-Learning programmes of study at EUC. The Unit supports both students and academic staff of EUC's E-Learning programmes, by ensuring quality access to educational materials and technological resources. Students receive initial instruction in the use of the educational platform from the DEU, as well as ongoing advice. If issues arise with the technology or delivery of their courses (not the academic content), then they bring these up with the DEU. The DEU also coordinates with other administrative structures of the university, such as the Office of the Vice Rector of Academic Affairs, the Department of Information Systems and Operations, the Department of Enrollment, and the Registrar's Office. Its mission is to ensure that e-learning is a vital element in all aspects of the university's academic and administrative policies and actions. As an administrative structure, the DEU does not get involved in the academic running of E-Learning programmes. These are the responsibility of the Schools and Departments through the programme coordinators. Rather, the	Choose level of compliance:

	DEU facilitates their smooth operation. It is Schools, Departments and E-Learning programme coordinators that secure the quality assurance processes and academic support for E-Learning programmes under the relevant procedures and structures of the Office of the Vice Rector of Academic Affairs. The Committee on Internal Quality Assurance (C.I.Q.A.) which is headed by the Vice Rector of Academic Affairs has established a Standing Committee named the "Pedagogical Planning of E-Learning Programmes of Study Standing Committee". The Director of the DEU is an ex-officio member of the Committee. This Committee is involved in all internal quality assurance procedures and decisions related to the University's E-Learning programmes of study. The Committee's aim is to improve the learning experience of E-Learning students through its active and qualitative support of the University's E-Learning programmes of study and is responsible for supporting Schools, Departments and E-Learning programmes in: • monitoring and evaluating the existing E-Learning programmes of study; • the pedagogical planning of new E-Learning programmes of study; • the design and evaluation of educational material for E-Learning programmes of study; • the support and feedback processes to the students; • the pedagogical use of technology, internet and digital information; • the technical training and support of the instructors of E-Learning programmes of study; • the interaction between academic staff and students in the E-Learning programmes of study.	

	The Pedagogical Planning of E-Learning Programmes of Study Standing Committee is comprised of all E-Learning programme coordinators and three ex-officio members: • The Director of the DEU, responsible for coordinating the DEU administrative support processes it provides to Schools, Departments and E-Learning programmes; • The Chair of the Faculty Professional Development C.I.Q.A. Standing Committee, responsible for coordinating with the Pedagogical Planning of E-Learning Programmes of Study Standing Committee in deciding and offering trainings, seminars, and professional development support to all E-Learning instructors; and • The Chair of the Digitally Enhanced Learning (D.e.L.) C.I.Q.A. Ad-Hoc Committee, responsible for complementing the three sub-committees' actions in supporting the E-Learning instructors in utilizing the latest digital and online software and tools in their instruction. The following points deal with further issues relevant to the EEC's suggestion to set up differently the DEU and the way E-Learning programmes are supported: • All academic staff of the Departments and Schools teaching on E-Learning programmes have long experience of instruction in tertiary education and research in their fields. All instructors receive ongoing professional development and training in e-learning, particularly in the use of contemporary communication technologies for teaching and learning by the Faculty Professional Development C.I.Q.A. Standing Committee (through the procedures	

	presented above). The combination of instructors' proficiency in their discipline, prolonged experience in e-learning, combined with the modern infrastructure of EUC, aims to guarantee the quality of EUC's E-Learning programmes of study. • Educational materials are expressly designed to support and convey the learning content; they might also include other types of open educational resources and tools (either text, media, multimedia, digital documents, e.g. audible content, motion pictures, spreadsheets, photos, PDFs, graphics, etc. or material created by the students themselves), etc. EUC's pedagogical model is flexible and can be adapted to the special characteristics and objectives of each course. • Course instructional design is supported by the Office of the Vice Rector of Academic Affairs which employs a full-time Instructional Designer who assists, guides and coordinates all e-Learning instructors. The Instructional Designer has the support of the C.I.Q.A. sub-committees and receives feedback from the DEU in the production of training materials and courses via integrating the latest educational technologies, as the EEC suggests. By employing an Instructional Designer, the Office of the Vice Rector of Academic Affairs aims to raise the level of technological know-how available at EUC by supporting the e-Learning academic staff with the design of educational resources and material of an interactive and engaging nature based on contemporary instructional design principles. All academic staff offering e-Learning courses are assisted on learning	

	resources development processes of their courses. Furthermore, they receive professional support and advice on the development and revision of their curricular material, and the development of courses according to EUC academic quality standards so that all facets of the students' learning experience can be ensured. The support is provided on-site, via telephone calls and online. Thus, academic staff are able to enhance the learning experience of e-Learning students, including the ways they provide learning resources in Blackboard Learn Ultra, the way they deliver short videotaped lectures on various topics, interactive asynchronous activities for their students, ways of using formative assessment, and the ways they (re-) organize their e-learning courses or the materials. Finally, the Instructional Designer, along with another two staff members (a video-producer and a technology expert), runs a video production in-house studio under the name "Content Factory Studio". This is the facility where e-Learning instructors develop their own short video learning materials. "Content Factory" is an EUC initiative under the office of the Vice Rector of Academic Affairs aiming at producing high-value, well-organized materials for students in various courses, supported by professionally produced videos that are produced on campus in EUC's own video studio. The ultimate purpose of the "Content Factory" initiative is to further enhance the learning experiences of our students. • E-Learning students are guided and supported in all their academic activities by the instructors teaching	

	in the E-Learning programmes of study. Course instructors provide students tutoring and mentoring on the content of their courses, their evaluation and assessment. The course instructors are in charge of the teaching and learning process of each course. They provide students with all the necessary information and resources for the delivery of the course. They are also responsible for the students' evaluation, as well as for the management of the learning content. • In addition, in alignment with relevant CY.Q.A.A. guidelines and open/online universities' international practices, for each course a Course Coordinator is appointed. Their role is to coordinate the course in case there are more than one section regarding issues of content, design and elaboration of the learning activities, procedures and student evaluation. Moreover, the Programme Coordinator is the person in charge of the structure and the content of each programme, as well as for resolving conflicts between instructors and the students or between the students and the administrative services of the University. • Students are also supported by Student Advisors and the members of the Distance Education Unit who counsel them on administrative related issues, the planning of their study, problem resolution, and decision-making issues (e.g. course selection and enrolment, registration and payment of tuition fees, etc.). Modification of the provisions presented above are periodically discussed by the	

	Academic and Administrative Leadership of the University and are assessed based on the impact this would have on the quality of services provided and its added value before any implementation takes place.	
5.2 Given the increasing significance of distance learning programmes, it is essential to address the latest trends in educational technology and online learning in a professional manner. This includes developing open educational resources, utilising learning analytics, and incorporating artificial intelligence applications, e.g., chatbots for academic guidance and student counselling.	We comply with these EEC recommendations. At EUC, educational material is expressly designed to support and convey the learning content; it might also include other types of open educational resources and tools (either text, media, multimedia, digital documents, e.g. audible content, motion pictures, spreadsheets, photos, pdfs, graphics, etc. or material created by the students themselves). EUC's pedagogical model is flexible and can be adapted to the special characteristics and objectives of each course. Instructional design support is supported through the Office of the Vice Rector of Academic Affairs which employees a full-time Instructional Designer who supports and coordinates all e-Learning instructors with the support of the C.I.Q.A. sub-committees and the feedback received by the DEU in the production of training materials and courses via integrating the latest educational technologies, as the EEC suggests. Through employing an Instructional Designer, the Office aims to raise the level of technological know-how available at EUC by supporting the e-Learning academic staff with the design of educational resources and material of an interactive and engaging nature based on contemporary instructional design principles. All academic staff offering e-Learning courses are assisted in learning resources development processes of their courses; receive professional support and advice on the development and revision of their curricular material,	Choose level of compliance:

	and the development of courses according to EUC academic quality standards so that all facets of the students' learning experience can be ensured. The support is provided on-site, via telephone and online, thus the academic staff to be able to enhance the learning experience of e-Learning students, including the ways they provide learning resources in Blackboard Learn Ultra for their students, the way they deliver short videotaped lectures on various topics, interactive asynchronous activities for their students, ways of using formative assessment, and the ways they (re-)organize their e-learning courses or the materials. Finally, the Instructional Designer alongside a video-production expert and a technology expert run a video production in-house studio under the name "Content Factory Studio" for e-Learning instructors to develop their own short video learning materials. At EUC, we have been researching different ways to utilise learning analytics form the Blackboard LMS platform, as well as the Students First Dashboard. Global Galileo Education (GGE) has been developing for some time now a portal that exports data from our courses to present them visually in a user-friendly way to the instructor of each course. This initiative is under the project name Student First Dashboard (SFD). EUC has been part of this effort and the D.e.L. Committee and the Department of Information Systems and Operations have been participating in this initiative for more than a year. SFD is focused on accessing and using analytics from students' participation in the E-learning courses offered in all E-learning programmes. Finally, it is important to note that the Blackboard Learn Ultra platform has an	

	incorporated AI (chatbot) solution which currently is only available to clients based in North America. Blackboard informed EUC that they have plans on expanding the coverage of their chatbot solution to other areas of the world. As soon as this is done, we will be able to utilise this chatbot, train it with the necessary data to be able to be used for academic guidance and student counselling.	
5.3 In light of recent developments in the area of generative AI tools such as ChatGPT, the university should issue a policy or guidelines, as well as training on how to use (or not use) such tools for teaching, learning and assessment.	EUC is committed to its academic staff professional development on the latest developments in teaching and instruction in tertiary education. Hence, the Faculty Professional Development C.I.Q.A. Standing Committee has already offered two developmental workshops on AI developments as follows: • Artificial Intelligence (AI) in Higher Education (20.2.2023); • Navigating the Opportunities and Threats of AI Tools in Education (14.3.2023); please find these in the 2022-2023 FPD full programme (Appendix VIII). In addition, the Faculty Professional Development C.I.Q.A. Standing Committee has taken the following decisions for the academic year 2023-24 and future steps: 1. A set series of five (5) different professional development modules for all instructors will be created and will be available for all faculty. This will be a collaboration between the Faculty Professional Development C.I.Q.A. Standing Committee and the Digital Enhanced Learning (D.e.L.) C.I.Q.A. Standing Committee. An indicative list of the modules appears below: a. Using AI to Improve Teaching.	

	b. Navigating AI and Academic Integrity. c. Leveraging AI for Effective Course Material Development. d. Enhancing Academic Assessment with AI-Assisted Assignment Grading. e. Creating Engaging Visual Materials and Presentations. 2. A small group of instructors (to be set up as an ad-hoc committee) will work throughout the Fall 2023 Semester to identify issues that need to be addressed through a policy. The instructors will review other universities' policies, but also will evaluate the application of a draft proposed policy points during their teaching throughout the semester. 3. By the beginning of the Spring 2024 semester, a policy will be submitted to C.I.Q.A. to be then approved by the Senate and immediately be used throughout the university.	
5.4 Students said that sometimes – especially the external lecturers – do not turn on their webcams, probably due to network capacity problems. EUC has to assure that external, part-time faculty members operate from a work setting with proper internet connectivity.	Based on the EEC recommendation a new university wide internal regulation was established in July by the Senate (97th Meeting, 25.7.2023) which builds on previous C.I.Q.A. decisions on the matter and addresses the EEC concerns. The Internal Regulation reads as follows: "*Cameras support interactiveness and it is therefore* ***compulsory*** *for all academic staff offering E-Learning courses or is involved in online instruction to have their cameras on during the whole duration of any teleconference/session/online activity with their students. Academic staff may use the EUC background screen developed by the Department of Operations and Information Systems or*	Choose level of compliance:

	any other screen they wish during their online sessions. *Based on the same local, European and international standards and guidelines, C.I.Q.A. clarifies that the same does not apply to students participating in teleconferences/sessions/online activities. For students what applies is the guidelines in the document "The EUC E-Learning Programmes of Study" prepared by the "Pedagogical Planning of E-Learning Programmes of Study C.I.Q.A. Standing Committee". The document is intended primarily for all academic staff involved in course design and teaching on the E-Learning programmes of study at European University Cyprus and introduces the essential elements of the pedagogical principles and teaching philosophy employed on all E-Learning courses at EUC. The document clarifies that students are **encouraged**- and not obliged- to have their cameras on during their online teleconferences/ sessions/online activities, and particular when they switch on their microphone to speak either to the instructor or their student mates. Thus, a culture of interactiveness is nurtured."*	

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:

B. 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 evaluation processes with the	Choose level of compliance:

	promotion process (please see our response in item 3.2). In closing, we are grateful to the EEC for their suggestions and insightful comments with regard to the Master in Cybersecurity E-Learning programme.	

C. Higher Education Institution academic representatives

Name	*Position*	*Signature*
Dr. Yianna Danidou	Programme Coordinator	
Dr. Ioannis Michos	Chairperson, Department of Computer Science and Engineering	 Ioannis michos (Aug 7, 2023 10:29 GMT+3)
Prof. Panagiotis Papageorgis	Dean, School of Sciences	 Panagiotis Papageorgis (Aug 7, 2023 08:48 GMT+3)

Date: 7.8.2023

5 Lemesou Avenue, 2112, Nicosia
T: + 357 22 504 340
F: + 357 22 504 392
e-mail: info@dipae.ac.cy

European University Cyprus

Appendix I

SYLLABI

Course Title	Introduction to Cybersecurity				
Course Code	CYS600				
Course Type	Compulsory (must be must be taken during the first semester of registration)				
Level	Master (2nd cycle)				
Year / Semester	1st Year/1st Semester				
Teacher's Name	Dr Yianna Danidou				
ECTS	10	Lectures/week	None	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 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 defense • Classify and describe different potential routes for cyber-attacks. • Understand 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	E-Learning
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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Communications and Network Security				
Course Code	CYS615				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year/1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	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. • Analyse networking methods and applications in practical systems. • Classify and describe different types of wired network attacks. • Classify and describe different types of wireless network attacks. • Describe and evaluate methods and devices used to protect networks.				
Prerequisites	None	Co-requisites	CYS600		
Course Content	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. Principles: the network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Network Attacks: scanning, malware, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-middle, session takeover, wiretaps, MAC table flooding, ARP poisoning, ICMP attacks, DNS poisoning, smurf and fraggle attacks, phishing, spam, war-dialling, methods to prevent the network attacks that have been covered (within the discussion of each attack type). Wireless Attacks: Encryption and key management vulnerabilities, wireless sniffing, war-driving, mobile/cellular cell spoofing,				

	eavesdropping, mobile phone attacks, methods to prevent the network attacks that have been covered (within the discussion of each attack type). General protection, prevention and detection: Firewalls and packet filtering, demilitarized zones (DMZ), intrusion detection and prevention systems, IPsec, VLANs and network zoning, MAC access control, network authentication, system hardening, encryption, authentication, universal threat management (UTM), web filtering, honeypots, awareness. Cloud security - definitions pertinent to cloud computing, identify risks, and delve into a security architecture, data protection, access management, monitoring, compliance, and emerging trends. Network management as an effective information-gathering tool and starting point for comprehensive protection mechanisms, use of network and asset management tools to ensure uniform conformity to relevant cybersecurity standards and policies. 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	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Cryptography				
Course Code	CYS625				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year/1st Semester				
Teacher's Name	Dr Nikos Tsalis				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	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.				
Prerequisites	None	Co-requisites	CYS600		

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	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
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	Examinations	50%
	Assignments/On-going evaluation	50%
		100%
Language	English	

Course Title	Cybersecurity Policy, Governance, Law and Compliance				
Course Code	CYS630				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year/2nd Semester				
Teacher's Name	Dr Yianna Danidou				
ECTS	10	Lectures / week	None	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	CYS600		

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	E-Learning
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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Cybersecurity Architecture and Operations				
Course Code	CYS645				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year/2nd Semester				
Teacher's Name	Dr Nikos Tsalis				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	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.				
Learning Outcomes	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.				
Prerequisites	None	Co-requisites	CYS600		
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), indicatiors 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	E-Learning
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* *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Ethical Hacking and Penetration Testing				
Course Code	CYS655				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 2nd Semester				
Teacher's Name	Dr Konstantinos Vavousis				
ECTS	10	Lectures / week	None	Laboratories / week	None
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	CYS600		

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	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.
Bibliography	*Kim, P. The Hacker Playbook 3: Practical Guide to Penetration Testing.* *Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. and Williams, T. Gray hat hacking: the ethical hacker's handbook. McGraw-Hill Education.* *"Hacking: The Art of Exploitation, 2nd Edition", by Jon Erickson*

	“Social Engineering: The Art of Human Hacking”, by Christopher Hadnagy and Paul Wilson *IEEE/ ACM/ Elsevier/ Springer Journals and Magazines*
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Cyber Threat Intelligence (CTI)				
Course Code	CYS660				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year/1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	3 Hours / 14 weeks	Laboratories / week	None
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	CYS600
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	E-Learning As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.		
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	Examinations	50%
	Assignments/On-going evaluation	50%
		100%
Language	English	

Course Title	Management of Communication and Leadership in High Stress and Crisis Situations				
Course Code	CYS665				
Course Type	Elective				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year/1st Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	3 Hours / 14 weeks	Laboratories / week	None
Course Purpose and Objectives	Smaller or larger catastrophes are happening at an organizational or national level all the time. Effective prevention and management is based on leadership and communication before, during and after the crisis situation. Community engagement can only be achieved through effective risk and crisis communication. The course will focus on risk communication, targeting different audiences, based on stress and crisis situations to which they are exposed, identifying the source of their vulnerability, as well as the methods for identifying and communicating appropriate solutions to the target audience(s). In particular, this course will focus on developing leaders who can navigate high-stress environments, make critical decisions, and communicate with clarity, empathy, and confidence to inspire their teams and stakeholders. The course will also focus on leadership with an aim to provide to the students, advanced knowledge and practical skills to effectively lead and communicate during times of intense pressure, uncertainty, and crisis.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Analyze the root causes and consequences of past cybersecurity incidents to inform incident response strategies. • Differentiate between various communication methods and their effectiveness in crisis situations. • Assess the efficiency and effectiveness of cybersecurity incident response teams in simulated scenarios. • Critique the clarity and effectiveness of crisis communication messages during mock cyber crises. • Judge the ethical implications of cybersecurity incident response actions and communications. • Design comprehensive cybersecurity incident response plans tailored to different types of cyber threats.				

<table>
<tr><td></td><td colspan="3">

Develop crisis communication protocols and messages for specific stakeholder groups.
Construct strategies to foster a resilient and adaptive cybersecurity workforce.

</td></tr>
<tr><td>Prerequisites</td><td>None</td><td>Co-requisites</td><td>CYS600</td></tr>
<tr><td>Course Content</td><td colspan="3">
Understanding the Incident:

Introduction to crisis situations and high-stress environments
Key principles of effective communication and leadership during crises
Standardizing language for optimized communications
Common terms in crisis management and incident response
Analyzing the lifecycle of a cybersecurity incident
Differentiating between incidents and crises in the cybersecurity context
Case studies of major cybersecurity incidents and their implications

Defining Objectives for Incident Management

Establishing clear objectives for the Incident Management (IM) group
Retaining focus and maintaining clarity during busy and intense situations
Identifying critical success factors for effective crisis leadership

Initial Information Gathering

Techniques for gathering timely and accurate information during crises
Analyzing and evaluating data from different sources
Utilizing tools and technologies for information collection and analysis

Delegating Tasks and Team Management

Delegating initial tasks to the crisis response team
Utilizing the "IM Starting Grid" from the Cyber Incident Response Tool Kit (CIMTK)
Coordinating concurrent activities among support teams (IR, IT, HR, Legal, etc.)

Assessing and Building the Crisis Management Team

Evaluating the composition of the crisis management team
Identifying required skills and expertise for crisis response
Fostering collaboration and synergy among team members

Building the Communications Plan

Developing a comprehensive crisis communication plan
Tailoring communication strategies for different stakeholders

</td></tr>
</table>

	• Addressing legal and regulatory considerations in crisis communication Interacting with Different Stakeholders • Identifying and prioritizing stakeholders in cybersecurity incidents • Tailoring communication for technical and non-technical audiences • Building trust and credibility with stakeholders during crises • Handling media and public relations during cybersecurity incidents • Techniques for effective communication with internal and external stakeholders • Handling media and public relations during crises • Navigating communication challenges with different audiences Cybersecurity Incident Response Management • Developing and implementing an incident response plan • Coordinating cross-functional cybersecurity incident response teams • Managing resource allocation and task delegation during incidents • Lessons learned and continuous improvement in incident response Psychological Aspects of Cybersecurity Incidents • Understanding the psychological impacts of cyber incidents on teams and individuals • Supporting employees' mental health and well-being during crises • Stress management techniques for cybersecurity professionals • Building a resilient cybersecurity workforce Tracking and Documentation • Importance of tracking activities, tasks, and communications during crises • Implementing tools and systems to monitor progress and updates • Creating clear and concise documentation for post-incident analysis Talking to or Working with the Attackers • Understanding the importance of dialogue with attackers during cyber incidents • Exploring options for engaging with attackers to gain time for remediation • Factors influencing response options and the decision-making process Tracking the Incident, Tasks, People, and Progress • Techniques for effective incident tracking and management • Utilizing incident tracking tools and software • Tracking incident information, progress, and response tasks Remediation of Network and Data Damage

	• Categorizing damage caused by attackers and prioritizing remediation efforts • Mapping remediation tasks to vulnerabilities to ensure comprehensive recovery • Addressing both on-premises and cloud-based solutions in the remediation process Secrets in Stolen Data and Systems • Identifying and handling sensitive information included in stolen data • Assessing the potential impact of exposed secrets on future operations • Strategies for safeguarding sensitive information in the future Reporting and Documenting the Case • Creating comprehensive incident reports encompassing both Incident Response and Incident Management aspects • Outsourcing certain aspects of the report to relevant stakeholders • Ensuring a structured and informative report for future reference and analysis Planning the Closure of the Incident • Determining which remediation tasks should be transitioned to non-incident mainstream projects • Conducting reflection meetings to capture root causes and lessons learned • Developing strategies for smooth incident closure and post-incident analysis Developing the Wider Team • Training non-IR and IM staff to improve awareness of cybersecurity issues • Techniques for enhancing the capabilities of the broader team to handle future incidents • Exploring tabletop exercises as a training tool and how to conduct them effectively
Teaching Methodology	E-Learning
Bibliography	Communicating in Risk, Crisis, and High Stress Situations: Evidence-Based Strategies and Practice, Vincent T. Covello ISBN: 978-1-119-02743-0 January 2022 ISO/IEC 27035 Information Security Incident Management

	NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide	
Assessment	Examinations	50%
	Assignments/On-going evaluation	50%
		100%
Language	English	

Course Title	Master Thesis				
Course Code	CSE670				
Course Type	Compulsory (for students choosing the Master Thesis) Optional (for students choosing the elective courses)				
Level	Master (2nd cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	Dr Ioannis Michos				
ECTS	30	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	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, regardless of the student's subfield of study (as long as it is in the general field of Computer Science). It 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. Finally, it aims to prepare the student for independent work as a recipient of a Master's degree.				
Learning Outcomes	Upon successful completion of this course students should be able to: • Demonstrate written and oral technical research skills. • Select and justify a research topic, and use various resources to carry out a literature search. • Design, execute, interpret and report results from empirical research projects. • Manage a project and explain the relevant techniques and tools needed in order to complete it successfully on time and within budgeted resources. • Identify real-world problems 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, and plan and manage their work. • Evaluate a proposed solution and prove its worth to the client. • Critically evaluate the project and the proposed solution, as well as recognize and describe legal, social or ethical obligations stemming from the project.				
Prerequisites	Consent of Instructor		Co-requisites	CYS600	
Course Content	Part A: Research Methods: The nature of research: Definitions and types of research; research process; topic selection and scope; feasibility and value.				

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.

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 report.

Part B: Thesis:

The student selects a topic from the Thesis Topics Catalogue which becomes available on the first day of the first week of the semester. Students receive the catalogue via a personal email sent to them by the course instructor, and they are also available on the departmental website. Once the students receive the topics, they have two weeks (by the second Friday of the semester) to choose a topic. Topics are assigned on a First-Come, First-Served basis, given that the students have passed all the pre-requisite courses for a specific topic. Once a topic is selected and agreed upon with the associated supervisor, the course follows the weekly breakdown structure as that is provided in the study guide. See Master Thesis study guide for further details.

The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. The roles and responsibilities are outlined below:

Student:

- To identify and scope a suitable problem
- Explain the value of the research
- To plan and control the project
- To carry out the necessary work
- To review and evaluate the work done
- To prepare and present the project deliverables
- To initiate and maintain contact with the academic supervisor

Academic Supervisor:

- To comment on the suitability of the selected project
- To discuss the mapping of the project onto the course requirements
- To discuss and approve the intended deliverables

	• To suggest starting points for consideration of background research • To discuss the nature of the thesis and comment on early drafts • To provide advice on issues associated with the project such as design, implementation, and proof of concept as appropriate. • To attend any presentation or demonstration of the project **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	E-Learning
Bibliography	Any material suitable for the subfield in which the student is undertaking the thesis will be specified by the instructor. Howard, K. & Sharp, J.A., The Management of a Student Research Project, Gower Turk, C. & Kirkman, J., Effective Writing: Improving Scientific, Technical and Business Communication, Chapman & Hall J. Zobel., Writing for Computer Science, Springer. W. Navidi, Statistics for Engineers and Scientists, McGraw-Hill Science/Engineering/Math; Latest Edition. Statistical Methods for Engineers, by Geoffrey Vining and Scott M. Kowalski, Thomson, Brooks/Cole, Latest Edition. J.G. Paradis, M., Zimmerman,The MIT Guide to Science and Engineering Communication, The MIT Press. D. Madsen, Successful Dissertations and Theses: A guide to graduate student research from proposal to completion, Jossey Bass. 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	**ASSESSMENT STRATEGY:** The specific deliverables for each individual's project must be discussed and decided upon in consultation with the academic and industrial supervisors. However, each project must involve deliverables falling into the following general categories: (a) A proposed solution to a real-world problem. (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 field. (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: • Project justification including its relationship to the current state of the art 10% 20 marks • Ability to select and use appropriate methods and techniques 10% 20 marks • The clarity, coherence and succinctness with which the solution is developed 30% 60 marks • Novelty. Does the work improve significantly the current state of the art? 30% 60 marks • Ability to critically review the project and assess its implications for future work in view of the project recommendations and conclusions 10% 20 marks • Project Management: Ability to plan and control the project 10% 20 marks _____ _____ 100% 200 marks In addition, students are reminded about presentation issues: Is the document format (including spelling) of good quality? Is it well organized into appropriate sections? Is the style of language used appropriate for an academic report?

	ASSESSMENT: Written Thesis: 80% Oral Presentation 20%
Language	English

Course Title	Research Methods				
Course Code	CSE600				
Course Type	Optional				
Level	Master (2nd Cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	none	Laboratories / week	none
Course Purpose and Objectives	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.				
Learning Outcomes	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				
Prerequisites	None	Co-Requisites	CYS600		
Course Content	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				

	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	E-Learning
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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Special Cybersecurity Topics				
Course Code	CYS670				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Dr Imre Lendak				
ECTS	10	Lectures / week	None	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 • Understand 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	CYS600
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	E-Learning
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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Cybersecurity Risk Analysis and Management				
Course Code	CYS675				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	Dr Nikos Tsalis				
ECTS	10	Lectures / week	None	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	CYS600		
Course Content	Introduction: Definition of cybersecurity risk and associated terminology, the position of risk analysis and management in relation to the other components of a cybersecurity programme.				

	Principles: Assets, vulnerabilities, threats, threat actors, likelihood. Management of risks compared to simple acceptance. Risk treatment options: avoidance, mitigation, transfer, acceptance. Assets: 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. Vulnerabilities: 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. Threats: 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. Risk analysis: 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. Risk management: 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	E-Learning
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* *"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up"*, by Evan Wheeler

	"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	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Data Privacy in the era of Data Mining and AI				
Course Code	CYS680				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	Dr Yianna Danidou				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide a comprehensive overview of growing data privacy threats to future communication technologies and Internet of Things (IoT) applications such as the Smart Grid and Smart Cities, e-Health and Wireless Sensor Technologies. Recent advances in the technical ICT fields of pervasive communications, combined with the science of big data mining and machine learning, are continuously transforming the way we interact with each other, with physical devices and infrastructures. Such technologies are becoming more tightly intertwined with our daily activities and we are becoming more integrated into the cyber-physical systems that surround us. The positive (economic) impact on society of such advances is enormous; however, big data information flows exposes important privacy details of our daily lives and our behavioural patterns. Such information may potentially be abused for purposes ranging from digital identity theft to targeted marketing, or discrimination based on medical history or other digital footprints, leading to fundamental privacy concerns. On this basis, the objectives of this course further include: a) Understanding interdisciplinary aspects of data handling and cyber security solutions: ultimately, this involves modelling and defining the trade-off between privacy and utility in information sharing IoT scenarios, in a mathematically rigorous way. b) Familiarise with fundamental data mining and machine learning algorithms with a focus on their application as privacy-invasive technologies. c) Learn how to develop application-specific privacy enhancing techniques, including security layers such as intrusion detection, privacy-by-design methods, and privacy-aware sensing.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Discuss privacy-by-design principles. • Get an overview of EU legislative and business regulatory aspects of data handling.				

	• Use cyber security protocols to engineer holistic data privacy system solutions. • Apply fundamental data mining and activity recognition algorithms to run privacy-invasive security tests. • Understand the principles of differential privacy and implement privacy-preserving algorithms. • Design privacy solutions for IoT scenarios, including Smart Grid, Smart Cities and wearable sensor technologies.		
Prerequisites	None	Co-requisites	CYS600
Course Content	IoT scenarios and privacy concerns: Smart meter data collection, wearable and smartphone mobile sensing technologies, data handling and data linking potential risks and system-level analysis. Mathematical privacy metrics and privacy invasion tools: relative entropy, mutual information, cluster classification, regression analysis, residual features, activity recognition, non-intrusive appliance load monitoring, exploratory data mining, differential privacy and atypicality. Cyber-security privacy protection solutions: anonymisation with trusted third party, data aggregation, data splitting, secure multi-party communication protocols, homomorphic encryption, zero-proof cryptosystem, data obfuscation, physical behaviour optimisation. Anonymity networks (e.g. Tor and I2P), ethics Information-theoretic privacy preserving techniques: privacy-utility trade-off optimisation, privacy-aware data sensing, lossy data compression, rate-distortion function, differentially private billing. General Data Protection Regulation (GDPR) Standardisation, regulatory and business aspects: consent-based approaches, ethical aspects of data collection, access control restrictions, business requirements and risks. ISO/IEC 27001 family of standards. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on the practical privacy scenarios and IoT considerations.		
Teaching Methodology	E-Learning		
Bibliography	Keith M Martin, Everyday Cryptography: Fundamental Principles and Applications. Oxford University Press. Brij Bhooshian Gupta, Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. R. Mendes and J. P. Vilela, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications," in IEEE Access, vol. 5, pp. 10562-10582.		

	Clarence Chio, David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms. Dua, S. and Du, X., Data mining and machine learning in cybersecurity. Auerbach Publications IEEE/ ACM/ Elsevier/ Springer Journals and Magazines
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English

Course Title	Incident Response and Forensic Analysis				
Course Code	CYS685				
Course Type	Optional				
Level	Master (2nd cycle)				
Year / Semester	2nd Year/3rd Semester				
Teacher's Name	Dr Dimitrios Baltatzis				
ECTS	10	Lectures / week	None	Laboratories / week	None
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. An incident is a matter of when, not if, a compromise or violation of an organization's security will happen. If the organization has a mature incident response capability, they will have taken measures to ensure they are prepared to address an incident at each stage of the process. Today's cyber threats have become very complex and require additional resources and skills to mitigate detect analyze and respond to. The uniqueness and complexity of these threats is often beyond the capabilities of ordinary IT teams. Detecting these incidents therefore requires additional skills such as forensics, malware analysis and threat detection which help decipher how these threats operate and therefore how they can be prevented and mitigated. Forensic analysis techniques are introduced, along with standard tools that are used to carry out computer forensic investigations, with emphasis on digital evidence acquisition, handling and analysis in a forensically sound way. Digital forensics serves as the mechanism for understanding the technical aspects of the incident, potentially identifying the root cause, and discovering unidentified access or other malicious activity				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Understand Incident Response • Managing Cyber Incidents • Define and describe the main phases of incident response • Evaluate incident data and indicators of compromise (IOC) to determine the correct responses to an incident • Identify different kinds of attacks methods to counter their effects • Describe the different phases of incident response – preparation, identification, containment, eradication, recovery, follow-up • Explain the principles of evidence collection and the chain of custody • Contact an incident respond analysis • Identify and evaluate key forensic analysis techniques, collect evident data from the incident, Fundamentals of Digital Forensics,				

	Forensic Imaging, Analyzing Evidence, System Memory and System Storage • Describe the ways in which cybercrime investigations use forensic analysis and legal issues regarding evidence collection. • Contact a forensic analysis of the evidence. Examine and analyze the evidence • Writing the Incident Report		
Prerequisites	None	Co-requisites	None
Course Content	Introduction: Definitions of incident response and forensic analysis, relation of incident response to the rest of cybersecurity operations, incident response phases - preparation, identification, containment, eradication, recovery, follow-up, indicators of compromise (IOC), forensic analysis as an incident response tool and as support for cybercrime investigations, cybersecurity forensics principles. Preparation: Policies and procedures, incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis, threat intelligence, vulnerability management, penetration testing, digital forensics, incident ticketing systems, incident documentation templates. Identification: Detection, incident triage, information gathering and reporting, incident classification, indicators of compromise (IOC). Containment: Damage limitation, network segment isolation, system isolation, forensic backup and imaging, use of write blockers, temporary fixes, malware spread limitation. Eradication: Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, cooperation with forensic analysis to understand the attack fully. Recovery: Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process. Follow-up: Documenting lessons learned, preparatory activities for similar future incidents, technical training, process improvement. Digital Forensics Investigation Process: Applicable laws, investigation methodology, chain of custody, evidence collection, digital evidence principles, rules and examination process, first responder procedures. Technical forensics tools and techniques: Hard disks, removable media and file systems, Windows forensics, duplication/imaging of forensic data, recovering deleted files and hidden or deleted partitions,		

<table>
<tr><td></td><td>steganography and image forensics, log analysis, password crackers, network device forensics, packet capture analysis, email tracking, mobile forensics, investigation of attacks, common tools (Autopsy, FTK, etc.)

Business case study and lecture: Lecture by invited experts from the cybersecurity industry, including law enforcement. Discussion normally focuses on the practicalities and challenges of incident response and the ways in which forensic analysis contributes to successful cybercrime prosecutions.</td></tr>
<tr><td>Teaching Methodology</td><td>E-Learning
As this course has a major practical component, a major part of the student workload is based on participating and completing online lab exercises.</td></tr>
<tr><td>Bibliography</td><td>

“Practical Cyber Forensics”, Niranjan Reddy, Apress, 2019,
“Digital Forensics Basics: A Practical Guide Using Windows OS”, Nihad A. Hassan, Apress 2019
Digital Forensics with Kali Linux, Shiva V. N. Parasram, Second Edition, 2020 Packt Publishing
“Incident Response & Computer Forensics, Third Edition” by Jason T. Luttgens and Matthew Pepe
“Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder”, by Don Murdoch
“Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response”, by Leighton Johnson
“The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics”, by John Sammons
Investigating Windows Systems by Harlan Carvey, 2018 Elsevier
“Digital Forensics with Open Source Tools”, by Cory Altheide and Harlan Carvey
“Digital Forensics Processing and Procedures”, by David Lilburn Watson and Andrew Jones
IEEE Journals and Magazines

</td></tr>
<tr><td>Assessment</td><td>
<table>
<tr><td>Examinations both theory and practice</td><td>50%</td></tr>
<tr><td>On-going evaluation through assignments</td><td>50%</td></tr>
<tr><td></td><td>100%</td></tr>
</table>
</td></tr>
<tr><td>Language</td><td>English</td></tr>
</table>

European University Cyprus

Appendix II

"Cybersecurity (18 Months/90 ECTS, Master of Science)"-E-Learning

TABLE 1: STRUCTURE OF THE PROGRAM OF STUDY

DEGREE REQUIREMENTS	**ECTS**
All students pursuing the M.Sc. in Cybersecurity E-Learning 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**
CYS600	Introduction to Cybersecurity	10
CYS615	Communications and Network Security	10
CYS625	Cryptography	10
CYS630	Cybersecurity Policy, Governance, Law and Compliance	10
CYS645	Cybersecurity Architecture and Operations	10
CYS655	Ethical Hacking and Penetration Testing	10
Master Thesis OR Research Methods course and Two (2) Elective Courses		**30**
CSE670	Master Thesis OR	**30**
CSE600	Research Methods **and** Any two (2) of the following Elective Courses	10
Elective courses (only if Master Thesis is not selected)		**20**
CYS660	Threat Intelligence	10

CYS665	Management of Communication and Leadership in Disasters	10
CYS670	Special Cybersecurity Topics	10
CYS675	Cybersecurity Risk Analysis and Management	10
CYS680	Data Privacy in the Era of Data Mining and AI	10
CYS685	Incident Response and Forensic Analysis	10

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:.....

SECTION B:

(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

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

The EUC E-Learning Programmes of Study

A Note on this Document

This document is intended primarily for all academic staff involved in course design and teaching on the E-Learning programmes of study at European University Cyprus (EUC). The document introduces the essential elements of the pedagogical principles and teaching philosophy employed on all E-Learning courses at EUC. The document breaks down into the following sections:

1. Introduction to e-learning at EUC
2. The Distance Education Unit
3. The EUC e-learning pedagogical model
4. The main principles of e-learning:
    a. Learner-centred learning design
    b. Inclusive design
    c. Co-design
    d. Interactive and collaborative learning
5. Support for e-learning at EUC
    a. Learning resources
    b. Academic guidance and support
    c. Administrative support
6. The fundamental structure of EUC's E-Learning Courses
    a. Course structure
    b. Synchronous meetings
    c. Asynchronous communication
    d. Course assignments
    e. Final exams
7. Student assessment in E-Learning courses
8. Programmes' quality assurance

1. Introduction to e-learning at EUC

European University Cyprus (EUC) has always met the differing educational needs of society by using the most up-to-date tools. As part of this mission, since 2013, EUC has offered fully recognized E-Learning Bachelor's (undergraduate) and Master's (postgraduate) programmes of study. The aim is to provide access to education for as many people as possible, particularly those who may not have had otherwise the chance to attend a programme of study.

Academic staff of the Departments and Schools teaching on E-Learning programmes of study have prolonged experience of instruction in tertiary education and research in their fields of study. All instructors receive ongoing professional development and training in e-learning, particularly in the use of communication technologies for teaching and learning. This combination of instructors' proficiency in their discipline, prolonged experience in e-learning, combined with the modern infrastructure of EUC, is what guarantees the quality of EUC's E-Learning programmes of study.

2. The Distance Education Unit

The Distance Education Unit (DEU) provides the administrative support for the E-Learning programmes of study of EUC. The Unit supports both students and academic staff of EUC's E-Learning programmes of study, by ensuring quality access to educational materials and technological resources. Students receive initial instruction in the use of the educational platform from the DEU, as well as ongoing advice, and if they have issues with the technology or delivery of their courses (not the academic content) then they bring these up with the DEU. The Unit also helps coordinate the production of training materials and courses, as well as coordinating with other administrative elements of the University, such as the Office of the Vice-Rector of Academic Affairs, the Department of Information Systems and Operations, the Department of Enrollment, and the Registrar's Office. Its mission is to ensure that e-learning is a vital element in all aspects of the University's academic and administrative policies and actions.

3. The EUC e-Learning Pedagogical Model

E-learning at EUC works according to a flexible pedagogical model that considers the needs of the student, the requirements of the discipline, and the technological infrastructure. It promotes best practice in instructional design and educational delivery, and provides useful guidelines against which instructors can assess their own educational practices.

This model follows the latest pedagogical guidelines and recommendations for the design and development of E-Learning programmes of study distributed by the Cyprus Agency of Quality Assurance and Accreditation in Higher Education (CY.Q.A.A.), including announcements of CY.Q.A.A. on 29.4.2020 and 4.5.2020 on E-Learning programmes of study, Study Guides and e-learning interactive activities. The model is regularly updated to ensure compliance with all requirements of the national framework. The EUC pedagogical model also takes into consideration the requirements and special characteristics of the legislation of countries other than Cyprus from which EUC E-Learning programmes of study have a large number of students (e.g. Greece), as well as the fundamental

functioning principles of the Open University of Cyprus, the Hellenic Open University, and other international Open Universities.

The **Blackboard Learn Ultra platform** is the environment that provides access to learning resources and content and supports the students' interaction with the material, their instructors and their classmates.

4. The main principles of e-learning

The EUC Pedagogical Model is based on the following learning principles:

- Learner-centred learning design
- Inclusive design
- Co-design
- Interactive and collaborative learning

Each of these principles are described below.

a. Learner-Centred learning design

The student holds a predominant position in the EUC pedagogical model. The entire process revolves around designing areas and resources to enable the student's learning. Information related to the E-Learning programmes of study are publicly available and objectives and expected learning outcomes of the courses as well as grading policies are available to all students and potential students. At the beginning of each semester, during the first meeting with students in courses, each instructor goes through her/his course outline and discusses with students the course content, learning process, activities and assignments. Students have the opportunity to make suggestions and customizations, bearing in mind that the fundamental content and objectives of the course cannot be altered as these were accredited by CY.Q.A.A. Meaningful learned-centred learning is also achieved by taking account of students' background, professional and prior education experiences, as well as taking advantage of opportunities for customization of the e-learning experience and learning activities based on students' own needs and interests. Finally, towards the end of each semester, students are asked to evaluate each of their courses online. Submission is anonymous and the time it takes to fill out the evaluation form is around 10-15 minutes. The survey pertains all aspects of the course and the overall learning experience of the student (hence named the Survey on 'Student Feedback on their Learning Experience' -SFLE), such as the course structure and content, the faculty performance, the facilities involved, the administrative support, etc. The information received are forwarded to faculty to review and act accordingly. The Chairperson of the Department also reviews the aggregated information per course and makes recommendations where needed.

b. Inclusive design

The inclusive design implementation of Universal Design for Learning (UDL) principles is one of the main concerns of the programme design and development

of all EUC programmes of study. The UDL principles in EUC's E-Learning programmes of study are implemented as shown in the table below:

UDL Principles	Activities and Course Design	Means, Technology and Tools
Provide options for Engagement	-Organisation of the course in weeks/themes/units with indicative timeframe for study -Facilitation of self-paced learning/study -Regular contact with instructor in a variety of ways -Assignments and learning activities linked to personal experiences, background, professional status, etc. (e.g. variations of practical experience, assignments linked to own experiences and work environment) -Compulsory and optional activities -Opportunity to choose some graded activities over others. -Options for individual and group activities and assignments -Options for authentic work (e.g. conducting small research projects in activities, assignments that avoid reproduction of literature but entail practical/implementation sections) -Variety in assessment methods (e.g. projects, portfolios, quizzes, open-ended questions, public dialogue discussions, discussion forum)	-LMS Blackboard Learn Ultra with accessibility features -Study guides available in various forms (word document, pdf) as well as content structured on platform follows the study guides -LMS build-in communication tools (e.g. discussion forums, chat options and messaging) -Options for communication off platform (e.g. blogs, personal IM, social network closed groups, video channels)
Provide options for Representation	-Alternative options of introduction of new knowledge and content (e.g. readings, teleconferencing, slide notes, pre-recorded videos, links to external content) -Both English and Greek literature (for programmes offered in Greek) -Uses of Glossary (in some courses that terminology is especially important) -Use of synchronous and asynchronous content connection activities (e.g. wikis, presentations, mind-mapping)	-Videos (accessible where possible) -Text on platform (online documents) -Visuals (e.g. diagrams, images, mind-maps) -Hyper-titles where possible -Recorded teleconferencing meetings available to all
Provide options for Action and Expression	-Synchronous and asynchronous options for interaction (student-student, student-instructor, student-content, student-platform) though various channels -Variety in assessment methods (e.g. projects, portfolios, quizzes, open-ended questions, public dialogue discussions, discussion forum)	-Interactive videos -Interactive (user-controlled) content (e.g. though authoring tools such as H5P) -Alternative accepted modes of communication (e.g. email, IM, discussion forum, chat, social media closed groups) -Alternative accepted modes of class participation (e.g. written, auditory, video presentations)

	-Variety of types of questions in final exams (by regulation all need to be written exams) -Creative assignments (e.g. presentations, repositories of resources, peer review activities) -Assignments broken in consecutive sections/parts during the semester (one building on the other)	-Access to Assistive Technology and reasonable adaptations through the Committee for the Support of Students with Disabilities and/or Special Educational Needs (Ε.Φ.Ε.Ε.Α.)

In addition to the above, inclusive e-learning design takes into consideration the students' workload (including assignments, examinations, learning outcomes and course literature) calculated in accordance with the ECTS of each course, and involves a variety of assessment methods that enable students to engage with and practice diverse skills and meet varying challenges. Various forms of written and oral examinations and assignments support the learner's general competencies. These include both individual and group work.

Where appropriate and possible, in order to ensure interconnections between theories and practice, syllabi comprise both theoretical and practical content; in particular, instructors are encouraged to develop assignments and examinations where students are required to use their experience gained from practice, in order to connect theory with practice. Finally, instructors provide support adjusted to students' individual abilities, learning needs and learning opportunities.

The University's annual Faculty Development Programme provides development training activities in inclusive design, as well as in differentiation and UDL in higher education.

c. Co-design

The instructors and the course coordinators, under the supervision and guidance of each program coordinator, regularly update their study guides to incorporate insights from ongoing training in learner-centred and inclusive design. Moreover, at the beginning and around the middle of the semester the program coordinator invites the instructors to a meeting to exchange opinions on students' issues and course delivery.

d. Interactive and collaborative learning

E-learning at EUC is designed in ways to promote interaction in various levels (learner-learner, learner-instructor, learner-content, learner-technology). The ultimate goal is to enhance the interaction between students and the learning that can only occur among motivated individuals working together. Interactive learning is a hands-on/real life approach to education founded upon building student engagement through guided social interaction connected with existing knowledge and their own experience and interests, with carefully designed and structured activities to facilitate learning in groups and challenge students to develop practical skills.

Interactive learning seeks to enhance the interaction between learners and:

1. the course materials
2. the instructor
3. their peers

Interactive learning emphasizes the active engagement of the learner in enrichment activities which aim at the practical and critical application of the theoretical knowledge. When interactive learning takes place within the contexts of student-material interaction, the student should be able to receive immediately feedback during her/his interaction with the course materials, and thus interactive learning will provide self-assessment opportunities. Interactive learning is, thus, a hands-on, real-life approach to education founded upon building activities to facilitate learning individually and/or in groups, challenging students to develop and apply practical scientific-specific skills and knowledge which are meaningful, connected to their existing theoretical knowledge, personal experiences, interests and (academic and professional) goals. The focal point of interactivity is always on the skills of learners, not the capabilities of the technology that seeks to facilitate learning.

Self-assessment and interactive exercises/activities are presented on a weekly basis. Such activities uphold the interest of students, motivate consistent participation and long-term engagement. Examples of such interactive exercises are the following:

- role playing
- simulations
- real-life scenarios
- learning tools
- online discussions for debating
- the use of visualization tools to come to a specific outcome
- brainstorming activities for answering a theoretical question
- problem-solving questions in groups
- preparing group PowerPoint presentations (e.g. after watching a video or studying a specific source)
- answering quizzes and peer reviewing assignments of other students, etc.

Gamification strategies are also embedded in EUC's E-Learning programmes of study. In addition, great emphasis is placed on communities of learning and collaboration. Learning collaboratively refers to using teamwork, through communication and discussion with the instructor and other student mates, to solve problems, develop projects, create products, either independently or jointly, etc. The construction of new knowledge is combined with the professional and personal experience of students, individual and group research processes and activities, knowledge management via the Blackboard Learn Ultra tools, etc. Collaboration is intertwined, supplemented and complemented with independent and autonomous learning, a necessary and needed condition of deep learning which is combined in a flexible way with other methodological approaches.

5. EUC support for e-learning:

Through guidance and support, each student receives personalized attention according to their needs, from the first day of their enrolment in an E-Learning programme of study. EUC supplies the following supportive structures and resources for students on their e-learning courses:

a. Learning resources

This can include educational materials expressly designed to support and convey the learning content, but it might also include other types of open educational resources and tools (either text, media, multimedia, digital documents, e.g. audible content, motion pictures, spreadsheets, photos, pdfs, graphics, etc. or material created by the students themselves), etc. EUC's pedagogical model is flexible and can be adapted to the special characteristics and objectives of each course.

b. Academic guidance and support

Students are guided and supported in all their academic activities by the instructors teaching in the E-Learning programmes of study. Course instructors provide tutoring and mentoring on the content of student's courses and their evaluation and assessment. The course instructor is the person in charge for the teaching and learning process of each course. They provide students with all the necessary information and resources for the delivery of the course. They are the persons responsible for the students' evaluation, as well as for the management of the learning content.

In addition, in alignment with relevant CY.Q.A.A. guidelines and respective open university international practices, for each course a Course Coordinator is appointed. Their role is to coordinate the course in case there are more than one sections regarding issues of content, design and elaboration of the learning activities, procedures and student evaluation.

The Program Coordinator is the person in charge of the structure and the content of each program, as well as for resolving conflicts between instructors and the students or between the students and the administrative services of the University.

c. Administrative support

Students are also supported by Student Advisors and the members of the Distance Education Unit who counsel them on administrative related issues, the planning of their study, problem resolution, and decision-making issues (e.g. course selection and enrolment, the registration and payment of tuition fees, etc.).

6. The fundamental structure of EUC E-Learning Courses

a. Course structure

Each course is carried out over 13 weeks, followed by a final exam week. Throughout the 13-week teaching period, up to six synchronous teleconferences are organised. The first of these is always scheduled for the first week of the semester after the orientation/familiarisation week (during which students become familiar with the **Blackboard Learn Ultra platform** and spend time studying the Course Outline and Study Guide of their courses); and the last is always scheduled in the last two weeks of the semester (always before the final examination week).

The rest of the synchronous teleconference dates are set by the instructor of each course in coordination with the students in order to best accommodate their availability and needs. Though Study Guides and the Course Outlines are structured in weeks, instructors are free to design and present their course content and activities in any way they consider useful to facilitate students' organization of their self-paced study, as well as to help students follow the Course Outline and learning objectives as communicated to them at the beginning of the course. This may maintain the weekly format, or follow a thematic organisation structure. In the case of thematic organisation, instructors should provide an indication of estimated week(s) of study, as well as matching with learning objectives and milestones of activities and course requirements during the semester.

b. Synchronous meetings

Teleconferences are set up using **Blackboard Collaborate** which is an embedded e-learning collaboration tool of the Blackboard Learn Ultra LMS platform. This virtual classroom tool enables instructors to create an engaging and pedagogically innovative environment for students fostering e-learning. During the teleconferences, the instructor, as facilitator and moderator, presents the main points of the topic under discussion, discusses with students related fundamental issues and provides guidance as to the content and materials to be studied at home by the students over the following weeks. Teleconference sessions may also include opportunities for synchronous group or individual work by students. All material is provided beforehand on the **Blackboard Learn Ultra platform**, so that students have a chance to study it, prepare questions on the content and activities of the specific weeks, and discuss these during the synchronous session that follows. The assignments and activities that are to be conducted asynchronously (approximate weekly study time is estimated at 10 hours – excluding assignment preparation time), are also discussed in these synchronous teleconferences. More importantly, through these teleconferences, interaction between the students and the instructor is achieved as students are given, among other things, the opportunity to ask questions or share reflections with other students and their instructor. The instructor also prepares interactive activities (please see relevant section above) to be prepared for and conducted during the synchronous teleconferences.

c. Asynchronous communication

During the semester, students communicate between themselves and with the instructor through the Blackboard Learn Ultra platform in an asynchronous form. The most common methods of asynchronous communication are by message, short chats and discussion forums. Messages are personal or group, sent through the platform and delivered as an email message to recipients' email inbox. Short chat discussions in Blackboard Ultra are enabled over assignments or other tasks assigned on the platform, and provide an opportunity for students to asynchronously exchange informal comments and ideas on any course item. Discussion forums can be either for general discussions (e.g. course inquiries), or assignment focused (graded or non-graded). For the latter, as appropriate per week or theme, students are engaged is collaborative activities and interaction such as discussion of particular course material. This material might have been

either independently studied, or presented and discussed in a videoconference synchronous learning meeting with the instructor.

d. Course assignments

For each course, students need to carry out individual and group assignments which are graded. The type and nature of each assignment is presented to students at the start of the semester through multiple avenues of communication on the platform, such as in the Course Outline and course Study Guides. It is also explained and discussed during the synchronous teleconferences (as described above). These graded assignments may require preparing an answer to a theoretical question (for instance, discussion of a quote from an academic article or judgment/position or discussion) which involves extended research, rational analysis, critical thinking and evaluation. Other graded assignments may include responding to a focus/problem question, which involves comprehensive understanding of focal content issues.

To increase student motivation and engagement, collaborative and interactive tools are used, such as Padlet for group participation and group projects, Flashcards, game-based learning (e.g. Kahoot & Archy Learning, Simulations, etc.), interactive videos and other interactive activities (e.g. though H5P integrated in the learning platform). This kind of assignments are used mainly for formative evaluation and aim to enrich student's knowledge and skills on the learning objectives of the topic. Specific assignment topics for each course are described in detail in the Study Guide of each course and posted on the Blackboard Learn Ultra platform, alongside evaluation rubrics for assignments including the grade weighting attached to each one. Through assignments, students conduct research on a specific topic using the online databases of the University library as well as other electronic resources, either individually and/or in groups (thus interacting with each other, with the material of the course, and with the instructor).

Apart from presenting their findings in a written form, students might elaborate on these during short oral presentations. These oral presentations are usually conducted asynchronously to be shared on the Blackboard Learn Ultra platform. There they can be viewed and commented on by fellow classmates, and evaluated by the instructor, as they form part of the overall grade ascribed to their assignments.

Even though variations across programmes of study exist, the approximate time for an individual assignment preparation is approximately 20 hours, for a group assignment preparation is approximately 15 hours and for preparing an oral presentation is approximately 5 hours.

When written assignments are submitted, these are automatically checked through Turnitin for plagiarism through performing a similarity check in available databases. Instructors may use also Turnitin as a pedagogical tool to help students improve the final draft of their assignment before the submission on the Blackboard Learn Ultra platform. Flags for instances of similarity constitute opportunities for formative feedback and opportunities for revision during the writing process.

Instructors proceed promptly (within 15 days at the latest) in providing the assignment grade as well as detailed feedback that the student needs to take into

consideration in a formative mode of assessment for his/her better preparation of the final exam. Feedback can be given either on an individual basis (especially for individual assignments), on a group basis (e.g. in the case of group assignments) or a whole class basis.

Blackboard analytics are also helpful for an evidence-based approach to teaching and learning, because they provide instructors greater insight into the factors that affect their students' performance. Analytics also provide a snapshot of what students know, what they should know and what can be done to meet students' academic needs.

During the semester, students are requested to work both individually and in groups in order to conduct their self-assessment and interactive exercises/activities, which are described in detail in the Study Guide of each course on the platform, and are presented on a weekly basis. At least three to five of such interactive activities/exercises are graded by the instructor (allocated a percentage of 10-15%). This element of the course further allows the students to engage in asynchronous interactive learning at three levels presented in the respective section above (approximate time for activities/exercises preparation is estimated at 30 hours).

e. Final exams

After the 13-week learning period is completed, students take the final exam for each of their courses (allocated percentage at 50%). The final exam assesses in a comprehensive way the level at which students have acquired the theoretical knowledge covered in the course, as well as the degree to which they have developed the skills in critical analysis aimed at by the course (approximate time for exam preparation 50 hours).

For the online/e-Proctoring implementation of the final exams of E-Learning courses, the LockDown browser platform **Respondus** is used. This tool allows the students to undertake their exams in a proctored environment. Before starting the exam, the students are asked to use their University IDs to identify themselves. Exam recorded videos are stored on GDPR compliant Amazon Web Services (AWS Servers) and are automatically deleted every two (2) months. Up until students have submitted their final answers, the software 'locks' their computer, not allowing them to perform any other actions on their PCs, other than their final examination, until they have submitted their final answers. The software uses the camera and microphone of the student's PC to monitor their movements, sounds, conversations, etc. and produces reports of student activity at the time of the examination. If potential transgressions are detected by the software, the instructor is alerted accordingly (i.e. the software flags specific snapshots and then the instructor when reviewing the recording can view those points more cautiously). The instructor, who is the only one with access to the recording, can access the video to review the reasons for a high alert. If deemed necessary, the student is interviewed and explanations for the alert are requested. If the information is not sufficient, further actions are taken based on the University's regulation on academic dishonesty. The University policy on penalties related to academic dishonesty is presented on instructors' Course Outlines for each course.

A video presentation of the semester delivery of a typical E-Learning course appears here:

MA_Ed_Sciences_SpecialandInclusive_DL_video.mp4

7. Student assessment in E-Learning courses:

The Study Guides provided at the beginning of the semester contain specific instructions, resource guidance, rubrics for grading, assigned grade value for graded activities, and timelines. Students prepare and deliver their work, including the final exam, aiming to accumulate a grade of at least 60% to pass an undergraduate class, or 70% to pass a graduate class. The grading system of E-Learning courses according to EUC regulations appears in the table below:

BACHELOR's DEGREES (UNDERGRADUATE PROGRAMMES)					MASTER's DEGREES (POSTGRADUATE PROGRAMMES)			
Grade	**Description**	**ECTS**	**Percentage**		**Grade**	**Description**	**ECTS**	**Percentage**
A	Excellent	4.0	90+		A	Excellent	4.0	90+
B+	Very Good	3.5	85-89		B+	Very Good	3.5	85-89
B	Good	3.0	80-84		B	Good	3.0	80-84
C+	Fairly Good	2.5	75-79		C+	Fairly Good	2.5	75-79
C	Average	2.0	70-74		C	Average	2.0	70-74
D+	Below Average	1.5	65-69		D+	Below Average	0	
D	Poor	1.0	60-64		D	Poor	0	
F	Failure	0			F	Failure	0	
I	Incomplete	0			I	Incomplete	0	
W	Withdrawal	0			W	Withdrawal	0	
P	Pass	0			P	Pass	0	
AU	Attendance	0			AU	Attendance	0	
TR	Course from transfer	0			TR	Course from transfer	0	

For every week the objectives and learning outcomes are clearly stated in all Study Guides, allowing students to self-assess progress by reflecting on their grasp of target concepts and knowledge. Based on each assignment specific criteria, an indicative grading rubric is included in the Study Guides. An example of a rubric for a group research paper in a research methodology course appears below:

Group Assignment Evaluation	Criterion	Maximum points possible	Points Earned
Names:			
Literature review and theoretical framework	• adequate presentation of basic theoretical tools • adequate presentation of local and international literature on the topic • presentation of researcher's epistemological paradigm • justification of necessity and importance of study	4	
Methodology	Justified presentation and bibliographic documentation of the	8	

	methodological choices concerning all parts of the methodological design: • appropriate research problem statement and research questions • data collection methods • participant profile • sampling and recruitment method • data analysis method • data collection duration • ethics issues • validity and reliability strategies		
Analysis-interpretation	• adequate interpretation and presentation of the findings • with documentation with original excerpts from the data, and • documentation from the literature	8	
Conclusions	• link of basic conclusions to the literature • comprehensive discussion of basic conclusions	3	
General	• proficient use of language • appropriate use of APA • general presentation-appearance of the work	2	
Total points		**25**	

8. Programmes' quality assurance

In order to improve the learning experience for the students, EUC has established a Standing Committee under the University's Committee of Internal Quality Assurance (C.I.Q.A.) named the "Pedagogical Planning of E-Learning Programmes of Study Standing Committee". The Committee is involved in all internal quality assurance procedures and decisions related to the University's E-Learning programmes of study. The Committee's aim is to improve the learning experience of E-Learning students through its active and qualitative support of the University's E-Learning programmes of study and is responsible for supporting Schools in:

- monitoring and evaluating the existing E-Learning programmes of study;
- the pedagogical planning of new E-Learning programmes of study;
- the design and evaluation of educational material for E-Learning programmes of study;
- the support and feedback processes to the students;
- the pedagogical use of technology, internet and digital information;
- the technical training and support of the instructors of E-Learning programmes of study;
- the interaction between academic staff and students in the E-Learning programmes of study.

The composition of the Pedagogical Planning of E-Learning Programmes of Study Standing Committee for the academic years 2020-2022 is the following:

Chair	**Dr. Paraskevi Chatzipanagiotou,** Assistant Professor, Director of Distance Education Unit (Ex-Officio)
Members: School representatives	
School of Humanities, Social and Education Sciences	**Dr. James Mackay,** Assistant Professor **Dr. Maria Papazachariou**, Lecturer **Ms Petra Daniel**, Special Teaching Personnel
School of Sciences	**Dr. Yianna Danidou**, Lecturer **Dr. Constantinos Giannakou,** Lecturer **Dr. Costantinos Nikiforou,** Assistant Professor
School of Business Administration	**Prof. George Papageorgiou,** Professor **Dr. Lycourgos Hadjiphanis,** Assistant Professor **Dr. Onisiforos Iordanous,** Assistant Professor
School of Medicine	**Dr. Theodoros Lytras**, Assistant Professor **Dr. Kostas Gianakopoulos**, Assistant Professor
School of Law	**Dr. George Chloupis**, Lecturer
Ex-Officio Members:	
Chair of Digitally Enhanced Learning (D.e.L.) Ad-Hoc Committee	**Dr. Loucas Louca,** Associate Professor
Chair of Faculty Professional Development Standing Committee	**Dr. Eleni Theodorou,** Associate Professor

APPENDIX VI

English text follows

Οδηγίες για τα Εξ Αποστάσεως Προγράμματα Σπουδών του Ευρωπαϊκού Πανεπιστημίου Κύπρου

Αγαπητές Φοιτήτριες/Αγαπητοί Φοιτητές,

Η 3η Οκτωβρίου 2022 είναι η ημερομηνία έναρξης του Χειμερινού Εξαμήνου 2022 (F2022) και είναι σημαντικό να ενημερωθείτε για ορισμένα βασικά ζητήματα που αφορούν στο Εξ Αποστάσεως Πρόγραμμα που έχετε επιλέξει, καθώς και για τη συμμετοχή σας σε αυτό.

ΠΡΟΣΒΑΣΗ ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ ΤΗΛΕΚΠΑΙΔΕΥΣΗΣ BLACKBOARD LEARN ULTRA

Η διαδικασία διδασκαλίας και μάθησης λαμβάνει χώρα στο Virtual Campus, όπου χρησιμοποιείται η πλατφόρμα τηλεκπαίδευσης Blackboard Learn Ultra. Μπορείτε να συνδεθείτε στην πλατφόρμα τηλεκπαίδευσης εδώ https://myeuclogin.euc.ac.cy Με τη μετάβασή σας στην εν λόγω πλατφόρμα, θα σας ζητηθεί να καταχωρήσετε Όνομα Χρήστη (Username) και Κωδικό Πρόσβασης (Password).

Στο **Όνομα Χρήστη (username)** θα καταχωρήσετε τη διεύθυνση του ηλεκτρονικού ταχυδρομείου (email address) που έχει δημιουργηθεί για εσάς από το Πανεπιστήμιο και σας έχει αποσταλεί στο ηλεκτρονικό μήνυμα **"Your University Credentials"** με την ένταξή σας στο Πρόγραμμα.

Στον **Κωδικό Πρόσβασης (password)** θα βάλετε τον αρχικό κωδικό που σας έχει αποσταλεί μαζί με το λογαριασμό ηλεκτρονικού ταχυδρομείου στο μήνυμα University Credentials (ή τον νέο κωδικό σε περίπτωση αλλαγής του αρχικού).

Σε περίπτωση που ακολουθήσετε σωστά τις παραπάνω οδηγίες και, παρόλα αυτά, αντιμετωπίζετε πρόβλημα σύνδεσης με την πλατφόρμα τηλεκπαίδευσης, σας παρακαλώ να επικοινωνήσετε ηλεκτρονικά με το support@euc.ac.cy, το οποίο επιλαμβάνεται την επίλυση τεχνικών προβλημάτων σε σχέση με την πλατφόρμα τηλεκπαίδευσης. Σας παρακαλώ να μην επικοινωνείτε με τους/τις διδάσκοντες/ουσες ή το προσωπικό της Μονάδας Εξ Αποστάσεως Εκπαίδευσης, επειδή δεν είναι οι αρμόδιοι να σας βοηθήσουν, και θα σας παραπέμψουν εκ νέου στο support@euc.ac.cy, με αποτέλεσμα να χαθεί πολύτιμος χρόνος.

ΠΛΟΗΓΗΣΗ ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ ΤΗΛΕΚΠΑΙΔΕΥΣΗΣ BLACKBOARD LEARN ULTRA

Με τη σύνδεσή σας στην πλατφόρμα τηλεκπαίδευσης **Blackboard Learn Ultra**, θα μπορέσετε να δείτε τις εικονικές τάξεις (e-classes) των μαθημάτων που έχετε επιλέξει. Περισσότερες πληροφορίες και καθοδήγηση σχετικά με την πλατφόρμα, μπορείτε να δείτε στον παρακάτω σύνδεσμο: https://euc.ac.cy/en/online-learning-transition-students/
Συνημμένο και στον σύνδεσμο που ακολουθεί το εγχειρίδιο 'Blackboard Learn Ultra για Φοιτητές':

Blackboard Manual (GR)

ΑΞΙΟΛΟΓΗΣΗ ΤΩΝ ΜΑΘΗΜΑΤΩΝ

Το 50% της τελικής βαθμολογίας αντιστοιχεί στις βαθμολογούμενες Εβδομαδιαίες Ασκήσεις Αυτοαξιολόγησης/Διαδραστικές Δραστηριότητες και στις Εργασίες που λαμβάνουν χώρα και θα υποβάλετε κατά τη διάρκεια του εξαμήνου, ενώ το υπόλοιπο 50% αντιστοιχεί στην τελική εξέταση.

Οι **τελικές εξετάσεις** θα πραγματοποιηθούν **για τα προπτυχιακά και τα μεταπτυχιακά προγράμματα σπουδών στις 20-22 Ιανουαρίου 2023**.

ΣΗΜΑΝΤΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΕΧΕΤΕ ΥΠΟΨΗ ΣΑΣ

Το παιδαγωγικό μοντέλο εκπαίδευσης στα εξ αποστάσεως προγράμματα σπουδών του Ευρωπαϊκού Πανεπιστημίου Κύπρου περιστρέφεται γύρω από ένα ενιαίο κεντρικό στοιχείο: τον/την εκπαιδευόμενο/η και την υποστήριξή του/της στο δρόμο για τη μάθηση. Για την υποστήριξή του/της, απαραίτητη προϋπόθεση αποτελεί η σωστή προετοιμασία των δραστηριοτήτων μάθησης. Σε αυτές επιδρούν άμεσα τέσσερα θεμελιώδη στοιχεία, τα οποία βρίσκονται πάντα παρόντα στην εκπαιδευτική διαδικασία, έστω και με διαφορετικό επίπεδο έντασης και συμμετοχής κάθε φορά. Τα στοιχεία είναι η **συνεργασία** (μεταξύ φοιτητών/τριών και φοιτητών/τριών-διδασκόντων/ουσών), η **καθοδήγηση** και η **υποστήριξη** (από το ακαδημαϊκό προσωπικό και το διοικητικό προσωπικό αντίστοιχα), και τα **μέσα** (περιβάλλον μάθησης, περιεχόμενα, εργαλεία, κτλ.).

Τα εξ αποστάσεως προγράμματα σπουδών του Ευρωπαϊκού Πανεπιστημίου Κύπρου βασίζονται τόσο σε σύγχρονη όσο και σε ασύγχρονη επικοινωνία, ώστε ο καθένας/καθεμία από εσάς να οργανώνει τη μελέτη του/της σύμφωνα με τις ανάγκες του/της. Κατά τη σύγχρονη επικοινωνία δίνεται η δυνατότητα στους/στις φοιτητές/τρειες να παρακολουθήσουν τις τηλεσυναντήσεις που διοργανώνει ο/η διδάσκων/ουσα, να αλληλεπιδράσουν με τους/τις συμφοιτητές/τριές τους και να επιλύσουν άμεσα τυχόν απορίες (σημειώνεται ότι οι τηλεσυναντήσεις βιντεοσκοπούνται και μπορούν οι φοιτητές/τριες να τις παρακολουθήσουν και ετεροχρονισμένα). Η ασύγχρονη επικοινωνία μέσω των εργαλείων της πλατφόρμας διασφαλίζει την εναρμόνιση της επίτευξης των μαθησιακών στόχων με το προσωπικό πρόγραμμα του/της καθενός/καθεμιάς σας.

Στις e-classes στο Blackboard Learn Ultra θα βρείτε αναρτημένα το διάγραμμα του κάθε μαθήματος, τον οδηγό μελέτης, το βασικό εγχειρίδιο (ή/και αναγνώσματα). Επιπρόσθετα για κάθε εβδομάδα του εξαμήνου αναρτώνται δημοσιεύσεις/σημειώσεις/υποστηρικτικό υλικό/ασκήσεις που αφορούν στο θεματικό περιεχόμενο της εβδομάδας. Σκοπός του οδηγού μελέτης είναι να διασφαλίσει την προσδοκώμενη αλληλεπίδραση μεταξύ των φοιτητών/τριών, των φοιτητών/τριών και του/της διδάσκοντα/ουσας, καθώς και των φοιτητών/τριών με το υλικό μελέτης. Πρόκειται για ένα μη στατικό αρχείο το οποίο δυναμικά μπορεί να αναβαθμίζεται/προσαρμόζεται/διαφοροποιείται με ανανεωμένες πηγές, εργασίες, δραστηριότητες, κ.ά. Το μαθησιακό υλικό για όλες τις εβδομάδες του κάθε μαθήματος περιγράφεται πλήρως και περιλαμβάνει σειρά από ηλεκτρονικές αναφορές, τις οποίες ο/η φοιτητής/τρια μπορεί να επισκεφθεί μέσω της ηλεκτρονικής βάσης δεδομένων

της βιβλιοθήκης του Πανεπιστημίου. Επιπρόσθετα, καταγράφονται τα κριτήρια αξιολόγησης και αυτοαξιολόγησης των εργασιών και δραστηριοτήτων. Παράκληση να δίνετε ιδιαίτερη σημασία στο υλικό που αναρτούν και παραπέμπουν οι διδάσκοντες/ουσες.

Από τη θέση της Διευθύντριας της Μονάδας Εξ Αποστάσεως Εκπαίδευσης, είμαι στη διάθεσή σας οποιαδήποτε στιγμή για να σας στηρίξω και να σας βοηθήσω σε ό,τι και αν χρειαστείτε κατά τη διάρκεια αυτών των εβδομάδων. Για την ταχύτερη εξυπηρέτησή σας, θα ήθελα να σας πληροφορήσω ότι:

- Για θέματα που αφορούν στο **περιεχόμενο των μαθημάτων**, παρακαλώ να επικοινωνείτε με **τους/τις διδάσκοντες/ουσες και τους/τις συντονιστές/στριες των μαθημάτων**. Στοιχεία επικοινωνίας τους υπάρχουν στο Διάγραμμα Μαθήματος του κάθε μαθήματος.
- Για **ακαδημαϊκή υποστήριξη**, παρακαλώ να επικοινωνείτε με τον/τη **Συντονιστή/τρια του προγράμματός σας**. Τα στοιχεία επικοινωνίας του/της μπορείτε να τα βρείτε από την ιστοσελίδα του Πανεπιστημίου ή τη γραμματεία της Σχολής, η οποία προσφέρει το Πρόγραμμα.
- Για τις **επιλογές** των **μαθημάτων** σας ανά εξάμηνο, παρακαλώ να επικοινωνείτε με το/τη **Σύμβουλο Φοιτητών (Student Advisor)** σας.
- Για **τεχνικά ζητήματα** (π.χ. σύνδεση στην πλατφόρμα, κωδικοί πρόσβασης, κτλ.), παρακαλώ να επικοινωνείτε με το support@euc.ac.cy.
- Για ζητήματα που αφορούν την **Επιτροπή για Φοιτητές με Ειδικές Εκπαιδευτικές Ανάγκες (Ε.Φ.Ε.Ε.Α.)**, παρακαλώ να επικοινωνείτε με το efeea@euc.ac.cy.
- Για **βεβαιώσεις φοίτησης ή/και αναλυτική βαθμολογία**, παρακαλώ να επικοινωνείτε με την **κα Ρένα Αθανασίου** (R.Athanasiou@euc.ac.cy), την **κα Ελίνα Δραγατάκη** (E.Dragataki@euc.ac.cy) και την **κα Γκρέτα Ηρακλέους** (G.Erakleous@euc.ac.cy).
- Για θέματα που άπτονται των **τελικών γραπτών εξετάσεων**, παρακαλώ να επικοινωνείτε με την **κα Μελίνα Χριστοδούλου** (Me.Christodoulou@euc.ac.cy).

Είναι ιδιαίτερα σημαντικό να απευθύνετε τα μηνύματά σας στα κατάλληλα άτομα, ώστε να μην χάνετε χρόνο και να σας εξυπηρετούμε όσο πιο άμεσα και αποτελεσματικά γίνεται. Σας επισημαίνουμε ότι το Πανεπιστήμιο θα χρησιμοποιεί τη διεύθυνση ηλεκτρονικού ταχυδρομείου (που δημιουργήθηκε για εσάς) για την αποστολή πληροφοριών και χρήσιμων στοιχείων για τις σπουδές σας. Είναι επομένως ευθύνη του κάθε φοιτητή και της κάθε φοιτήτριας να ελέγχει το ηλεκτρονικό ταχυδρομείο του Πανεπιστημίου σε τακτική βάση.

Τελευταίο, αλλά σίγουρα εξαιρετικά σημαντικό είναι η επαφή σας με τις e-classes. Ανεξάρτητα πόσες δεσμεύσεις έχετε, αφού αποφασίσατε να συμμετάσχετε στο εξ αποστάσεως πρόγραμμα σπουδών, θα πρέπει να συνδέεστε τακτικά με την πλατφόρμα τηλεκπαίδευσης. Σε περίπτωση που δεν γίνεται αυτό, δεν θα μπορείτε να ανταποκριθείτε στις απαιτήσεις του μαθήματος.

Δρ. Παρασκευή Χατζηπαναγιώτου
Διευθύντρια της Μονάδας Εξ Αποστάσεως Εκπαίδευσης
Ευρωπαϊκό Πανεπιστήμιο Κύπρου

Instructions for the E-Learning Programs of Study
of European University Cyprus

Dear Students,

The instruction period for the Fall Semester (F2022) commences on October 3rd, 2022 and there are some important matters relating to your studies of EUC E-Learning programs of study that you have selected.

ACCESS TO THE E-LEARNING BLACKBOARD LEARN ULTRA PLATFORM

The whole teaching and learning process takes place on the Blackboard Ultra Learn platform, part of our Virtual Campus. You can log in to the Blackboard Ultra Learn platform by using the following link: https://myeuclogin.euc.ac.cy. Once you have clicked on the link, you will be asked for your Username and Password.

Your **Username** is the email address that the University has created for you, which was sent to your personal email with the subject **"Your University Credentials."** upon your induction in the program.

You will also be asked to enter your **Password** in the relevant field. This was provided in the same email as your Username (or the new password in case of change of the original).

If you follow the instructions correctly and you still have difficulties with your connection to the Blackboard platform, please send an email to the following email address: support@euc.ac.cy. This is the address for technical support on the Blackboard platform. You are kindly requested to avoid contacting your instructors or the Distance Education Unit staff on this issue, as they will not be able to assist you.

NAVIGATION/USING THE E-LEARNING BLACKBOARD LEARN ULTRA PLATFORM

When you connect to Blackboard Learn Ultra, you will be able to view the e-classes of the courses that you have selected. For more guidance regarding Blackboard, please click the link below: https://euc.ac.cy/en/online-learning-transition-students/

Attached and in the link below you can find the 'Blackboard Learn Ultra for Students' Manual:

Blackboard Manual (EN)

EVALUATION OF COURSES

50% of the final grade in each course corresponds to the graded Weekly Self-Assessment & Interactive Exercises/Activities and assignments that are submitted during the semester. The remaining 50% corresponds to the final exam.

The final examinations for the **Bachelor** and for the **Master Programs of study will take place between the 20th– 22nd of January 2023.**

IMPORTANT INFORMATION TO REMEMBER

The pedagogical model of EUC has one central element: supporting the student on their learning journey. The proper preparation of learning activities is essential for this support. Learning activities are directly affected by four fundamental elements, with a different level of intensity and participation each time. These elements are **collaboration** (between students and students-instructors), **guidance** and **support** (from the academic and the administration personnel respectively), and **resources** (learning environment, contents, tools, etc.).

European University Cyprus E-Learning programs of study are based on both synchronous and asynchronous communication, allowing each one of you to organize your study according to your needs and schedule. During **synchronous** communication you will have the opportunity to participate in teleconferences organized by the instructor, to interact with your classmates, and to resolve any questions immediately (it must be noted that the teleconferences are videotaped and students can watch them on a convenient time). **Asynchronous** communication employs the platform tools to ensure that each of you can achieve the learning goals of the class according to your personal schedule.

In the e-classes on Blackboard Learn Ultra you will find posted the course outline of each respective course, the study guide, the basic textbook (and/or readings). In addition, for each week of the semester, notes/supporting material/exercises/activities relating to the weekly topic are being posted. The aim of the study guide is to ensure that the expected interaction between students, student and instructor, student and the material is achieved. The study guide is a living document that will be updated/adapted/differentiated by renewing sources, exercises, activities, etc. The material for all weekly activities of each course is fully outlined and it includes electronic references, which the student will access electronically via the University's library. Moreover, criteria for the evaluation and self-assessment of the work of students are also defined. You are requested to pay special attention to the material given to you by your instructors.

As the Director of the Distance Education Unit, I am always available to support and assist you with everything you need. However, in order to receive a prompt and a more effective response/assistance, I would like to inform you of the following:

- For matters related to the **content of the courses**, please contact your **instructors**. Their contact details can be obtained from the Course Outline of each of your courses.
- For **academic support**, please contact the **Coordinator of your program of study**. Their details are available in the EUC website or from the Secretary of your School.
- For **choosing** your **courses** each semester, please contact your individual **Student Advisor**.
- For **technical matters** (e.g. connection to the platform, access codes, etc.) please contact support@euc.ac.cy.
- For the **Committee for Students with Special Educational Needs (C.S.S.E.N.)**, please contact efeea@euc.ac.cy.

- For **verification letters and transcripts**, please contact **Ms. Renne Athanasiou** (R.Athanasiou@euc.ac.cy), **Ms. Elina Dragataki** (E.Dragataki@euc.ac.cy) and **Ms. Greta Erakleous** (G.Erakleous@euc.ac.cy).
- For matters related to **final exams**, please contact **Ms. Melina Christodoulou** (Me.Christodoulou@euc.ac.cy).

It is very important that you direct your requests to the right people in order to assist you as swiftly as possible and prevent wasting your valuable time.

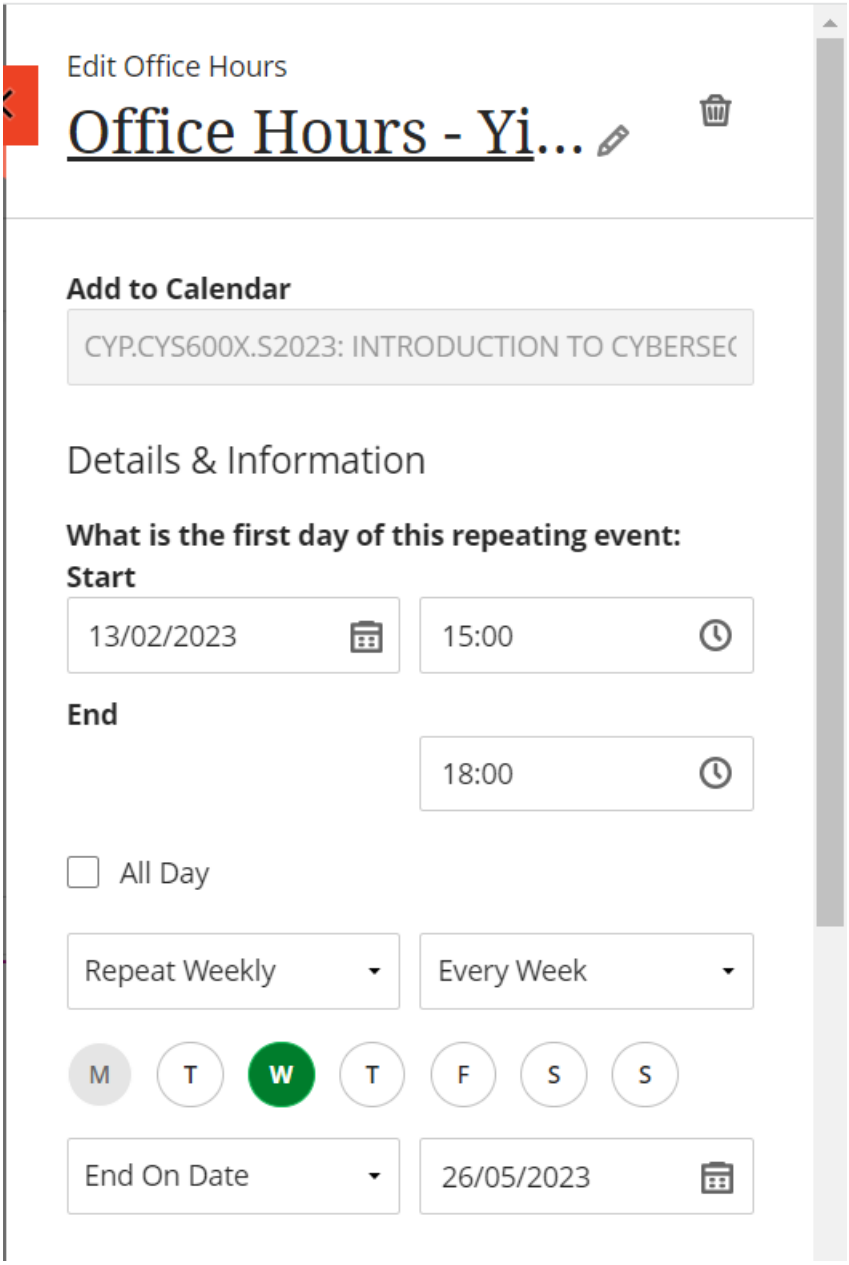
Note that the University will **only use your University email address** for contacting you with information relevant to your studies. It is each students's responsibility to check their University email regularly.

Finally, an extremely important note on e-classes; no matter how many commitments you have, since you have decided to join this program, you should connect to the Blackboard platform regularly in order to catch up. Failure to do so, will result in not meeting the requirements of the course.

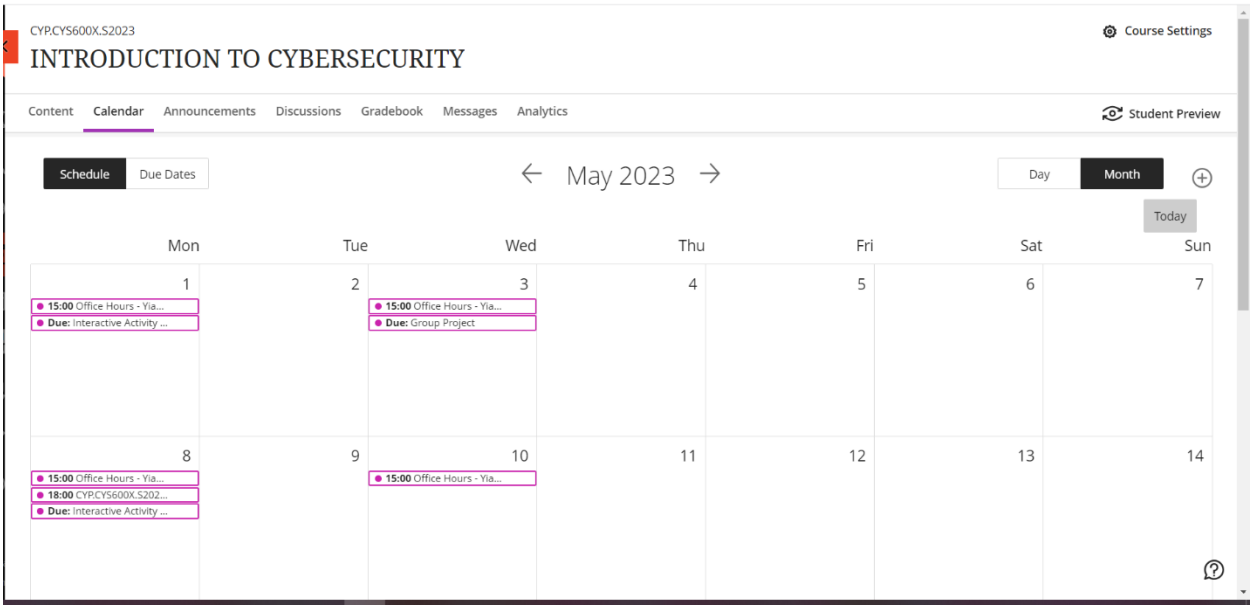
Dr. Paraskevi Chatzipanagiotou
Director, Distance Education Unit
European University Cyprus

Appendix VII

The following screenshot depicts the office hours that can be set by every instructor. As soon as these are set on Blackboard, the calendars of all students in the courses taught by the instructor will be updated to match the office hours set.



The calendar of each course is then updated to show all office hours, teleconferences set and deadlines.



European University Cyprus

Appendix VIII

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**	