



Doc. 300.1.2

Higher Education Institution's Response

Date: 13.04.2021

- **Higher Education Institution:**
University of Central Lancashire, Cyprus (UCLan Cyprus)

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

In Greek:

Μεταπτυχιακό στην Ασφάλεια Κυβερνοχώρου

In English:

MSc in Cybersecurity (1 year/ 90 ECTS, Master of Science)

- **Language(s) of instruction:** English
- **Programme's status:** Currently Operating



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 2019” [N. 136 (I)/2015 to N. 35(I)/2019].

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) must justify whether actions have been taken in improving the quality of the programme of study in each assessment area.*
- *In particular, under each assessment area, the HEI must respond on, without changing the format of the report:*
 - *the findings, strengths, areas of improvement and recommendations of the EEC*
 - *the deficiencies noted under the quality indicators (criteria)*
 - *the conclusions and final remarks noted by the EEC*
- *The HEI's response must follow below the EEC's comments, which must be copied from the external evaluation report (Doc. 300.1.1).*
- *In case of annexes, those should be attached and sent on a separate document.*



The School of Sciences and the MSc Cybersecurity team would like to express their sincere appreciation to the External Evaluation Committee (EEC) members for their well-targeted, comprehensive and valuable comments and recommendations towards enhancing our MSc Cybersecurity programme. We appreciate all the positive comments noted on the EEC's report, which inspire us to continue and strengthen our programme and current practices. We also appreciate the EEC's recommendations for improvement, which allowed us to further refine our programme and its market competitiveness.

We have considered and addressed all the EEC's recommendations for improvement, and in what follows, we provide our response to them along with any relevant information and actions taken.

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

(ESG 1.1, 1.2, 1.8, 1.9)

EEC REPORT

Findings for Cybersecurity (1 year/ ECTS, MSc)

The program is among the first Cyber Security programs in Cyprus. The program offers a comprehensive and well-motivated selection of modules on important security-related topics. The program content has been developed based on the current expectations for cybersecurity programs, academic profiles of the teachers as well as industry feedback. This program has different entry requirements compared to the MSc program in Computing.

Strengths for Cybersecurity (1 year/ ECTS, MSc)

The program covers important areas in cybersecurity and there appears to be a good balance between theory and practice. The program structure is actively developed and demonstrated by making the information warfare module optional in the new curriculum.

Common strengths for the three programs

The rapid response across all programs to the covid situation was noted and applauded.

The facilities represent the state of the art and provide excellent support for both education and research.

Areas of improvement and recommendations for Cybersecurity (1 year / ECTS, MSc)

This program has different entry requirements compared to the MSc program in Computing. The EEC recommends the harmonization of the entry requirements.

The program does not emphasize cryptography or the mathematical aspects of cybersecurity. These could be offered via an optional module to those students who have limited cryptography and mathematics background when starting the MSc. studies.

The content on the cyberwarfare module is useful and relevant however it may be worth looking at replacing this module with another which offers more practical training to students.

UCLAN CYPRUS RESPONSE

“This program has different entry requirements compared to the MSc program in Computing. The EEC recommends the harmonization of the entry requirements.”

The MSc Cybersecurity entry requirements have been amended as per the EEC recommendation and they are now aligned with all of our MSc programmes, and specifically MSc Computing. The only change to the existing entry requirements is to the following sentence:

Original Sentence: Applicants will need to have at least a Bachelor's degree (Higher Second Class of 2.1) or equivalent in a computing or closely-related discipline.

Updated Sentence: Applicants will need to have at least a Bachelor's degree (Lower Second Class of 2.2) or equivalent in a computing or closely-related discipline.

“The program does not emphasize cryptography or the mathematical aspects of cybersecurity. These could be offered via an optional module to those students who have limited cryptography and mathematics background when starting the MSc. studies.”

We agree with the recommendation of the EEC and we have included a new optional module on Cryptography to the programme. The description of the new module is available in Appendix A.

“The content on the cyberwarfare module is useful and relevant however it may be worth looking at replacing this module with another which offers more practical training to students.”

We agree with the EEC that the Cyberwarfare module is not as practical as other modules in the programme, but we believe that Cyberwarfare is an important subject area for some of our students. The objective of the module is to cover cybersecurity aspects at a national level, including cybersecurity aspects related to critical infrastructures, e.g. national cybersecurity strategies and policies, SCADA cybersecurity, Advanced Persistent Threat (APTs) strategies, etc. Students who enter the programme are often practitioners who work in national cybersecurity agencies, and in positions that require knowledge of cybersecurity at a national level as well as threats against critical infrastructures. Also, programme graduates have been employed in similar positions and they reported the value of the topics covered in the Cyberwarfare module. To this end, and as the Cyberwarfare module is optional, we would like to maintain it in the programme; therefore, it can be taken by students who have an interest in the subject area. It should be noted that the programme already includes another optional module that is more practical, the Incident Handling module, and it will be enhanced with one additional practical optional module on Cryptography (new module as per the EEC's recommendation). Moreover, given the EEC's comment that the Cyberwarfare module does not provide as much practical training as other modules, additional practical activities have been scheduled to be incorporated within the module's curriculum to further balance theory and practice.

2. Teaching, learning and student assessment (ESG 1.3)

EEC REPORT

Findings for the three programs

The Department establishes student admission criteria for each programme, which are adhered to. The three programs have excellent industry relevance, and the studies support professional certification. The number of students in the teaching rooms is suitable for theoretical, practical, and laboratory lessons. The teaching materials are up-to-date and of an appropriate standard.

The teaching staff of the Department seems to have regular and effective communication with their students and provide timely and effective feedback to their students. Students were very complimentary of access to staff and appreciate the criteria and the method of assessment as well as the criteria for marking being published in advance. The learning process is properly designed to achieve the expected learning

outcomes. The assessment allows students to demonstrate the extent to which the intended learning outcomes have been achieved.

The members of teaching personnel for each course have the relevant formal and fundamental qualifications for teaching the course, as described by the legislation including subject specialisation and publications within their respective disciplines.

Strengths of the three programs

The teaching staff of the Department seems to have regular and effective communication with their students and provide timely and effective feedback to their students.

The ratio of the number of students to the total number of teaching personnel is adequate for the support and safeguarding of the programme's quality.

The great majority of teaching is delivered by resident faculty that are employed on a full-time basis and all full-time staff have Ph.D. qualifications.

Areas of improvement and recommendations for the three programs

The university does not have an instrument for sabbaticals. The EEC recommends developing an instrument for enabling both short-term and longer-term research visits. In addition, inter-sectoral staff mobility with industry would appear to be beneficial in supporting the development and exchange of knowledge and skills building on the synergies between the academic environment and the industry.

The committee would encourage examination of the proportions of full-time faculty and adjunct faculty. The committee would welcome an increase in full-time faculty and their reduction in adjunct faculty, commensurate with the aim of increasing student numbers.

The EEC values the real-life industry relevance of the degree programs; however, recommends strengthening also the research connection of the M.Sc. degree programs.

Faculty research productivity is paramount. In order to facilitate this faculty-student contact hours should be monitored and perhaps reduced. Research output is a key parameter in global university rankings.

UCLan Cyprus does not have a Ph.D. program at the moment. A number of students have continued their Ph.D. studies at UCLan UK. The EEC recommends exploring the possibilities of a joint Ph.D. program with the UK campus. This could motivate research-oriented students to choose the M.Sc. programs at UCLan Cyprus. A Ph.D. program is a very necessary instrument for supporting research in general. This would necessitate dedicated research accommodation for the Ph.D. students. A critical mass of Ph.D. students would help the research student experience. Ph.D. students can help in running laboratories and guiding undergraduate/master's theses as part of the research training. The committee would encourage this.

UCLAN CYPRUS RESPONSE

“The university does not have an instrument for sabbaticals. The EEC recommends developing an instrument for enabling both short-term and longer-term research visits. In addition, inter-sectoral staff mobility with industry would appear to be beneficial in supporting the development and exchange of knowledge and skills building on the synergies between the academic environment and the industry.”

We agree with the EEC that an instrument for sabbaticals can be beneficial. Due to its young age, the School/University did not have a Sabbatical Scheme. To this date, the academics had opportunities for short-term and longer-term research visits through the many funded projects they are engaged in and which include research visits. Also, the University participates in the Erasmus+ programme, which funds short-term teaching and internship mobilities to other partner institutions. Already many of the School's –and the programme's– faculty have taken advantage of this and have participated in such mobilities that offer the opportunity to initiate discussions and exchange ideas on further research collaborations. Furthermore, depending on its available funds, the School often sponsors training or research visits for each faculty member. Nevertheless, we acknowledge the importance and benefits of a sabbatical scheme, especially in terms of providing additional opportunities for the academics to engage in short- or long-term research mobilities and activities, and thus, further enhancing our research environment. After the recommendation of the EEC during the evaluation visit, a request had been made at the University level to develop a sabbatical scheme for the University. This has already been drafted by the Senior Academic Management Team and it is currently awaiting approval by the University Senate (the draft is expected to be reviewed/approved during the next Senate meeting, on June 3rd, 2021). It is expected that the approved sabbatical scheme will be in effect by the new academic year.

We also agree with the EEC's recommendation that inter-sectoral staff mobility with industry can be beneficial. The School of Sciences fully supports such mobilities and until now, this was materialised primarily through Erasmus + mobilities with industry partners. Following the EEC's recommendation and the implementation of the new University Sabbatical Scheme, we anticipate that academics will have more opportunities to strengthen their engagement with the industry.

“The committee would encourage examination of the proportions of full-time faculty and adjunct faculty. The committee would welcome an increase in full-time faculty and their reduction in adjunct faculty, commensurate with the aim of increasing student numbers.”

As per the EEC comments, currently, the below is part of the strengths of the programme:

“The ratio of the number of students to the total number of teaching personnel is adequate for the support and safeguarding of the programme's quality.

The great majority of teaching is delivered by resident faculty that are employed on a full-time basis and all full-time staff have Ph.D. qualifications.”

The School (and the Programme) is committed to continue this good practice. Academic resources are reviewed at the School and programme level every year and necessary provisions/budgets are requested for the hiring of new academic staff as necessary. As the programme grows in terms of student numbers, we agree with the EEC that the hiring of new full-time faculty will become necessary and relevant actions will be taken.

“The EEC values the real-life industry relevance of the degree programs; however, recommends strengthening also the research connection of the M.Sc. degree programs.”

The MSc Cybersecurity curriculum is both, research and industry informed. Academics do a regular research and technology scouting, alongside their own research activities, integrating research and industrial project outcomes into the curriculum. Although the overall programme curriculum is updated yearly, on many occasions, specific learning material is updated during the academic year to cope with the dynamic nature of the threat landscape and relevant research and technological advances. For example, learning material was recently enhanced with legal and ethical scenarios from the EU funded CANVAS project, with outcomes from the Mitre ATT&CK project related to Advanced Persistent Threats activity, etc.

Furthermore, we would like to emphasize that MSc Cybersecurity students have the opportunity to conduct applied research in the context of their Master's Project (thesis), working on real world problems and contributing innovative solutions. Evidence of the quality of research work conducted by the students is the

scientific publications that resulted from their thesis work. Latest student-led research papers include the following:

- Chatzis, P., Stavrou, E. Cyber-Threats to Border Control Infrastructures, Computers & Security, Elsevier Journal, (under submission).
- Pierre, J., Stavrou, E. Towards Designing Advanced Password Cracking Toolkits: Optimizing the password cracking process, in Proceedings of ACM UMAP (User Modelling, Adaptation and Personalization), Adaptive and Personalized Privacy and Security Workshop, June 2019.

Moreover, students who are performing applied research are working towards the design and development of innovative open-source cybersecurity applications, which are shared on GitHub. The applications were demonstrated in 4 invited training sessions with participants from the industry and academia.

We would like to ensure the EEC that we greatly value research informed and industry informed teaching and we will continue working in this context, strengthening even further the research component in the MSc Cybersecurity.

“Faculty research productivity is paramount. In order to facilitate this faculty-student contact hours should be monitored and perhaps reduced. Research output is a key parameter in global university rankings.”

We agree with the EEC’s comment and we consider it vital for our academics to be productive in research. To ensure and support this, the School (and the University) operates an academic workload model, which as it was observed and noted by the EEC, follows an interactive process of defining the academics’ yearly workload and considers each academic’s individual plans. As a result, the workload model provides the necessary foundations and processes to be able to adjust the distribution of academics’ time between teaching, research and administrative duties. In summary, the workload model is prepared by all academics before the commencement of the academic year, and it is reviewed and discussed with the Head of School. The standard target distribution of the academics’ workload hours is 40% teaching, 40% research and 20% administration, but during the annual review, other adjustments can be made according to the academic’s research output and engagement. The workload model considers several aspects of the responsibilities of the academics on the aforementioned three areas, along with the time allocated to each. As a result, once the model is prepared, academics who are above the allocated 40% research active, can request a teaching reduction and increase in research allocation hours. It is the responsibility of the academic and the Head of School to ensure during the annual review meeting that academics are allocated the needed time to conduct research and be productive in this area. The workload model has been in operation for the last 6 years and it has proven very effective in assisting the School and the academics to keep a good balance between research, teaching and administrative work. It is a process we consider important for the sustainability and strengthening of our research environment, as well as for ensuring that teaching material is enhanced with the latest research developments, and as such, we are committed in continuing.

Moreover, as it was also observed by the EEC, all full-time academics of the MSc Cybersecurity programme are research active and many have ongoing high-quality publications in their field of expertise and have successfully received external research funding from international, national and internal funding sources and/or participated in international research projects. A list of publications (including high-impact journal publications, scientific monographs, conference publications including best paper awards, book, etc) as well as a list of externally funded research projects for each academic are available on the university’s website (www.uclancyprus.ac.cy).

“UCLan Cyprus does not have a Ph.D. program at the moment. A number of students have continued their Ph.D. studies at UCLan UK. The EEC recommends exploring the possibilities of a joint Ph.D. program with the UK campus. This could motivate research-oriented students to choose the M.Sc. programs at UCLan Cyprus. A Ph.D. program is a very necessary instrument for supporting research in general. This would necessitate dedicated research accommodation for the Ph.D. students. A critical mass of Ph.D. students

would help the research student experience. Ph.D. students can help in running laboratories and guiding undergraduate/master's theses as part of the research training. The committee would encourage this.”

The School of Sciences, and UCLan Cyprus in general, does not currently offer PhD degrees. Academics of the School act as PhD supervisors for PhD students from other Universities, primarily UCLan UK. The School is positive in offering its own PhD degrees and we believe that this will be an additional benefit to assist the School in further enhancing its research environment. The School will investigate this possibility and take necessary actions (e.g. validate new PhD programmes through UK and Cyprus Quality Assurance Agencies).

3. Teaching Staff

(ESG 1.5)

EEC REPORT

Findings for Cybersecurity (1 year/ ECTS, MSc)

The number of the teaching staff is adequate to support the programme of study. The teaching staff status is appropriate to offer a quality programme of study. The visiting staff number does not exceed the number of the permanent staff. There is sufficient evidence of staff on this programme linking their research to their teaching.

Promotion processes seem transparent and staff engage in professional and teaching skills training.

Strengths for Cybersecurity (1 year/ ECTS, MSc)

Many members of the staff are engaged in active cybersecurity research with good publications in security journals.

Strengths for the three programmes:

The committee applauds the programs for their close engagement with the companies; however, the counsel a judicious balance between training and education. It is noted that adjunct staff present with specialized industrial knowledge and expertise.

There is a wide range of assessment instruments used in delivering the modules.

Area of improvement for the three programs:

The committee applauds the programs for their close engagement with the companies; however, the counsel a judicious balance between training and education. It is noted that adjunct staff present with specialized industrial knowledge and expertise.

There is a wide range of assessment instruments used in delivering the modules.

Areas of improvement for Cybersecurity (1 year/ ECTS, MSc)

The content on the cyberwarfare module is useful and relevant however it may be worth looking at replacing this module with another which offers more practical training to students.

Area of improvement for the three programs:

The committee encourages the staff to continue with the production of high-quality research publications. In some cases, research output seemed to be declining given teaching work.

The committee noted a large number of optional modules, however, they recommend consideration of the associated curricula burden for faculty. While this effort is applauded the question remains as to the efficacy of maintaining modules with very low student numbers.

The committee recommends exploring the use of blended learning post-covid.

UCLAN CYPRUS RESPONSE

“The committee applauds the programs for their close engagement with the companies; however, the counsel a judicious balance between training and education. It is noted that adjunct staff present with specialized industrial knowledge and expertise.

There is a wide range of assessment instruments used in delivering the modules.”

We thank the EEC for the positive feedback with regards to the programme’s close engagement with the industry as well as the wide range of assessment instruments utilised within the programme.

“The content on the cyberwarfare module is useful and relevant however it may be worth looking at replacing this module with another which offers more practical training to students.”

This recommendation has been addressed in Section 1 and our response can be found in page 5.

“The committee encourages the staff to continue with the production of high-quality research publications. In some cases, research output seemed to be declining given teaching work.”

We would like to assure the committee that high quality research is an essential element of our academic work and as reported in Section 2 (page 8), the School operates an academic workload model which is prepared and reviewed on an annual basis and which aims to safeguard academic’s time to conduct research. It is true that research output may vary from year to year, depending on the research work an academic is working on, but it is definitely not overall declining. A list of publications for each academic is available on the university’s website (www.uclancyprus.ac.cy). The list includes high-impact journal publications, scientific monographs, conference publications including best paper awards, books, etc.

“The committee noted a large number of optional modules, however, they recommend consideration of the associated curricula burden for faculty. While this effort is applauded the question remains as to the efficacy of maintaining modules with very low student numbers.”

This comment is not applicable to the MSc Cybersecurity programme, as the programme only offers 3 optional modules (Cyber Warfare, Cyber Incident Handling, and Cryptography).

“The committee recommends exploring the use of blended learning post-covid.”

The team is happy to explore the possibility of continuing existing (covid related) and implementing new blended learning approaches for the programme post-covid, always within the guidelines and regulations of the CY QAA and UK QAA.

4. Students

(ESG 1.4, 1.6, 1.7)

EEC REPORT

Findings for the three programmes

In the three-degree programs, the students receive dual-degree certificates from UCLan Cyprus and UK, respectively.

Certification includes details on the degree structure, learning goals, and level of achievement. The degree program design has taken the ACM curriculum into account and the programs are aligned with industry certifications such as Cisco CCNA and the Linux professional curriculum. There are excellent synergies in administration functions, planning of teaching, and best practices with the UCLan UK. The students receive help and support from the administration regarding the admission and education-related forms and processes. The Admission Team is responsible for the processes. Approximately 30% of the B.Sc. students continue to the M.Sc. in Computing.

Strengths for the three programs

The student selection process is transparent, and the process is implemented in a consistent manner. Student study progress is monitored, and feedback is gathered on a systematic basis.

Areas of improvement and recommendations for the three programs

The student selection criteria differ between the Computing and Cybersecurity M.Sc. programs. The committee encourages the internationalization of the M.Sc. programmes.

The first-year CS curriculum seems relatively light. The committee note that this is a four-year degree program; however, it is felt that if further CS module could be introduced in the first year. One suggestion offered was the inclusion of a module offering glimpses of modules to be undertaken in subsequent years.

The programming courses start with imperative Java and object-oriented programming is introduced later. The committee invites the B.Sc. program to consider objects early versus objects late OOP learning strategy. The committee notes the current objects late strategy. Object-oriented concepts are, however, “informally” introduced in the games module in year two. Harmonization of these strategies would strengthen the programming modules.

The committee encourages the introduction of an AI module.

The committee noted a large number of optional modules; however, they recommend consideration of the associated curricula burden for faculty. While this effort is applauded the question remains as to the efficacy of maintaining modules with very low student numbers.

UCLAN CYPRUS RESPONSE

“The student selection criteria differ between the Computing and Cybersecurity M.Sc. programs. The committee encourages the internationalization of the M.Sc. programmes.”

This recommendation has been addressed in Section 1 and our response can be found in pages 4-5.

The programme design of MSc Cybersecurity considers a number of international curriculum standards. As such, the programme continuously strives towards its internationalization. We are in agreement with the committee for this recommendation and we will continue to work towards enhanced internationalization, both through research informed teaching and industry alignments.

The rest of the recommendations in this section are not applicable to the MSc Cybersecurity.

5. Resources

(ESG 1.6)

EEC REPORT

Findings for all three programs

The degree programs advocate student-centered learning and the programs have a relatively small number of students resulting in a favourable student-teacher ratio. The students appear to enjoy excellent tutoring and mentoring in the programs. Student satisfaction is a key performance indicator and the degree programs have attained top results in this metric. 75-80% of the graduates are being employed within three years. 83% of the students are reported to complete annual studies with very few interruptions or withdrawals.

The degree programs are based on modules. Students have a selection of optional modules depending on the degree program. The students are asked during the enrolment process what modules they plan to take. The B.Sc. and M.Sc. program does not have a significant overlap in the modules. The module offering is based on student participation and a module is not given if the quota is not reached. This results in unpredictability in terms of the modules that are given; however, the uncertainty is mitigated by estimating module popularity and also by the other programs sharing modules.

The staff is well aware of the quality assurance policy and it is an integral part of the everyday operations. The students benefit from a very good student-teacher ratio and student feedback is very positive.

Modules have been aligned with professional certification, such as Cisco CCNA and Linux professional curriculum.

Overall, the programs receive feedback from the industry and the graduating students appear to have excellent career prospects in the industry. The interviewed students emphasized the value of the degrees.

Strengths for Cybersecurity (1 year/ ECTS, MSc)

The program provides practice and industry-oriented cybersecurity education that is aligned with professional requirements. The program structure is versatile and involves the necessary laboratory and cloud-based experiments to promote an empirical understanding of cybersecurity topics. The modules and their key focus areas are relevant and interesting including IoT, industrial systems, ethical hacking, and information warfare. The program receives feedback from the industry regarding the topics.

Areas of improvement and recommendations for Cybersecurity (1 year/ ECTS, MSc)

It is recommended to develop the laboratory environment to be able to experiment with cloud-connected and cloud-based applications and services, for example considering Software Defined-Networks (SDN) and open cloud technologies such as OpenStack and container-based solutions.

The committee recommends the School to support 24/7 access to the laboratories.

UCLAN CYPRUS RESPONSE

“It is recommended to develop the laboratory environment to be able to experiment with cloud-connected and cloud-based applications and services, for example considering Software Defined-Networks (SDN) and open cloud technologies such as OpenStack and container-based solutions.”

We agree with the EEC’s recommendation and acknowledge the importance of cloud-connected and cloud-based applications and services. To this end, the programme team decided to embed new practical lab activities in the context of Cyber Defense (existing core module) to allow the students to experiment with cloud-based applications and services.

“The committee recommends the School to support 24/7 access to the laboratories.”

Through its annual monitoring, the School collects and considers students’ feedback, not only with regards to the delivery of programmes, but also with regards to School/University facilities, services and resources, including Library, IT, Laboratories and Student Support. Student access to laboratories is an area that was discussed extensively with the students and adjustments have been made through the years. For example, after the request of the students, an electronic system was developed through which students can check the availability of a laboratory, so that they can schedule their study time accordingly. Additionally, closer to assessment deadlines, access to laboratories is extended. Students can also request access to laboratories outside the normal hours of operation, depending on their needs.

We would also like to highlight that the MSc Cybersecurity programme operates online laboratories that can be accessed from anywhere and from any device (e.g. tablet, PC, laptop, etc.), providing flexibility to the students as to the online laboratories’ utilisation.

6. Additional for distance learning programmes

(ALL ESG)

Not applicable

7. Additional for doctoral programmes

(ALL ESG)

Not applicable

8. Additional for joint programmes

(ALL ESG)

Not applicable

Conclusions and final remarks

EEC REPORT

The EEC evaluated the School of Computing and the B.Sc. program in Computing, M.Sc. in Computing, and M.Sc. in Cybersecurity based on the provided accreditation reports and the remote site visit. The School and the three programs were found to have high standards and meet the quality expectations. Based on the materials and the site visit, the EEC has identified a number of areas in which the School and the three programs can make improvements to strengthening their profile and increasing impact.

UCLan Cyprus and the School of Computing advocate student-centered learning and the three evaluated programs have a relatively small number of students resulting in a favorable student-teacher ratio. The students appear to enjoy excellent tutoring and mentoring in the programs. There would seem to be a significant emphasis upon student learning support and the students themselves seem to both recognize and value such.

As a private university, there is a focus on education with an emphasis on degree programs that are self-sustaining in terms of finances. Thus the workload profile of the staff is teaching-oriented; however, research is an integral part of the strategy and the aspirations of the university, and while this is clearly evident an environment needs to be maintained that fully recognizes, measures and rewards research endeavor.

UCLan Cyprus has excellent synergies with UCLan UK at Preston. Joint planning of education appears to work very well. It is important that UCLan Cyprus continues to leverage resources and skills at UCLan Preston and conversely that UCLan Preston leverages emerging expertise at UCLan Cyprus. This relationship can prove mutually beneficial.

The EEC recommends to further leverage the synergies between UCLan Cyprus and UCLan UK while taking the challenges introduced by Brexit into account, for example differing privacy and other regulations. The joint delivery of education is a significant opportunity that should be explored, and which may yield critical mass in certain programmes and afford better economies of scale.

The School is focused on developing and improving the current programs. The EEC commends this strategy and encourages a strategy of managed growth of the School and its programs by leveraging the synergies with UCLan UK and developing programs based on the current strengths and perceived opportunity.

The assignment of duties follows the regular planning process and cycle of the university and the school. There is an annual meeting for reviewing workloads and preparing for the next academic year. The workload model is based on the 40-40-20 model, in which time is divided between education and research and with a smaller percentage with administrative duties. The assignment is interactive and takes into account the teacher's situation and plans.

Faculty research productivity is paramount. In order to facilitate this faculty-student contact hours should be monitored and perhaps reduced. Research output is a key parameter in the global university rankings.

The School of Computing has ambitions of increasing the student intake during the next years that requires the optimization of resources, especially balancing education and research activities. The School has significant potential in attracting more research funding from Horizon Europe. The integral connection with the UCLan UK can help in establishing more opportunities for international research activities and projects.

The School's three evaluated degree programs have high industry relevance and the studies support competence building by being aligned with industry certifications. The EEC values the real-life industry

relevance of the degree programs; however, recommends strengthening also the research connection of the M.Sc. degree programs.

The School would benefit from more systematic scientific and industrial feedback regarding the degree programmes helping to ensure academic relevance while anticipating near-future industry needs. The degree programs emphasize professional aspects in Computer Science and having a wider scope in this would make the degrees more relevant for the future needs of the industry. To this end, an industry advisory board is recommended as an instrument for supporting the longer-term development of the School and the degree programs.

UCLan Cyprus does not have a Ph.D. program at the moment. A number of students have continued their Ph.D. studies at UCLan UK. The EEC recommends exploring the possibilities of a joint Ph.D. program with the UK campus. This could motivate research-oriented students to choose the M.Sc. programs at UCLan Cyprus. A Ph.D. program is a very necessary instrument for supporting research in general.

The university does not have an instrument for sabbaticals. The EEC recommends developing instruments for enabling both short-term and longer-term research visits. In addition, inter-sectoral staff mobility with industry would appear to be beneficial in supporting the development and exchange of knowledge and skills building on the synergies between the academic environment and the industry.

UCLAN CYPRUS RESPONSE

The School of Sciences and the MSc Cybersecurity team would like to thank the EEC members for their valuable feedback towards enhancing our MSc Cybersecurity programme. The constructive discussions with the EEC members during the evaluation visit as well as the comments provided on the EEC report enabled our team to reflect on our existing practices and identify opportunities to strengthen them. We have addressed the EEC's recommendations, which we believe have significantly enriched our programme and improved its market appeal.

We strongly agree with the EEC's comment that research should continue being an integral part of our strategy and aspirations and we are committed to maintain and further strengthen our existing research environment, through the recognition, measurement and reward of research endeavours. As reflected in the School's vision, mission and strategy, this is an integral element for our future success and realisation of our long-term vision to be recognised as one of the premier science schools locally, regionally and internationally.

Regarding the collaborations with UCLan UK, the MSc Cybersecurity team enjoys a beneficial ongoing collaboration with the corresponding academic team in UCLan UK, and plans to continue its successful collaboration in terms of content design and delivery. As an example, the newly proposed module for Cryptography was designed in collaboration with the corresponding UCLan UK academic team. We appreciate the recommendation for exploring a joint delivery of education with UCLan UK colleagues and we are in agreement that it is a significant opportunity indeed. As we do across all academic areas, we will continue our excellent collaboration with UCLan UK, and as recommended, take further advantage of the synergies between the two campuses for the mutual benefit of the two Institutions, and specifically with regards to the sharing of resources for enriching the teaching and research environment. As indicated by the EEC, while the current Brexit situation introduces some challenges in the collaboration of the two Institutions, at the same time, it provides a number of new opportunities on which we can capitalise. Discussions are currently taking place between the two Institutions to ensure that both, challenges and opportunities, are considered and evaluated.

We are also in agreement with the EEC that academic workload should be closely monitored and adjusted (e.g. reduce teaching workload) for academics who are highly research active. As it was observed and noted by the EEC, the process of defining the academics' yearly workload is interactive and considers each



academic's individual plans, therefore it provides the necessary foundations and processes to be able to adjust the distribution of academics' time between teaching, research and administrative duties. This process is something we consider essential for the sustainability and strengthening of our research environment, and as such, we are committed in continuing. Moreover, as recommended by the EEC, a sabbatical scheme can be beneficial to allow academics further research mobilities and focus on research activities. To this end, a proposal has been made to the relevant University bodies, which responded positively. A sabbatical scheme for the University has been developed and it is currently on its final stages for approval (review/approval by the Senate). Offering our own PhD programmes is also another area of future development, which can support and enhance our existing research environment. As per the EEC's recommendation, this has been communicated to the University and discussion are currently taking place to explore the possibility of offering joint PhD programmes between UCLan Cyprus and UCLan UK, or independent PhD programmes by UCLan Cyprus.

With regards to the industry engagement with the School's programmes, as it is noted by the EEC, this is an integral part of our curriculum development process. Student employability is a key element embedded throughout all of our programmes, and to this end, we ensure that curriculum delivery combines research informed and industry informed teaching, which prepares graduates for diverse careers in the international market. As part of our efforts, through the years, we have established several strategically targeted industrial and academic partnerships, with depth and breadth, many of which resulted in providing students with enhanced knowledge and skills, parallel completion of professional certifications or professional body accreditations and recognitions, which are in high demand by the industry. We do note and agree with the EEC's recommendation to formalise the contribution of our industry partners to the School and its programmes, therefore all the necessary steps have been taken to form an Advisory Board for the School. We expect that our Advisory Board will be in place and active by the start of the new academic year.

B. Higher Education Institution academic representatives

Name	Position	Signature
Prof. Irene Polycarpou	Head of School of Sciences Chair of School of Sciences Academic Standards and Quality Assurance Committee	
Dr Eliana Stavrou	Course Leader of MSc Cybersecurity programme	
Dr Nearchos Paspallis	Deputy Head of School of Sciences Member of School of Sciences Academic Standards and Quality Assurance Committee	
Dr Kalypso Iordanou	Deputy Head of School of Sciences Member of School of Sciences Academic Standards and Quality Assurance Committee	
Dr Cosmina Theodoulou	Chair of Academic Standards and Quality Assurance Committee	

Date: 13.04.2021

Appendix A

Course Title	Practical Cryptography				
Course Code	CO4XXX				
Course Type	Optional				
Level	Level 7				
Year / Semester	Year 1/Semester 2				
Teacher's Name	Eliana Stavrou				
ECTS	10	Lectures / week	1 hours	Laboratories / week	2 hours
Course Purpose and Objectives	<p>The aims of this module are to:</p> <ul style="list-style-type: none"> • Provide an in-depth understanding of theoretical and practical aspects of cryptography. • Introduce cryptographic standards and best practices that students will most likely encounter as a security professional. • Identify which cryptographic protocols, tools, and techniques are appropriate for providing confidentiality, data protection, data integrity, authentication, non-repudiation, and obfuscation. • Provide an understanding of potential weaknesses and problems with ciphers and cryptographic protocols. • Apply symmetric and asymmetric cryptography and best practices as appropriate for a given scenario to achieve data protection. • Critically discuss cryptographic attacks and countermeasures. • 				
Learning Outcomes	<p>On successful completion of this module a student will be able to:</p> <ol style="list-style-type: none"> 1. Evaluate and compare theoretical and practical aspects of cryptography. 2. Research and report on cryptographic attacks and countermeasures. 3. Critically discuss and evaluate cryptographic controls for data protection. 4. Select appropriate techniques and apply them to solve a given problem. 				
Prerequisites	None	Required	None	None	None
Course Content					

Introduction

- History of cryptography
- Substitution ciphers, e.g. Caesar cipher, affine ciphers, etc.
- Transposition ciphers, e.g. reverse order, columnar cipher, etc.

Symmetric Encryption

- Block cipher design principles
- Block cipher operation
- DES, 3DES, AES, IDEA, etc.
- Stream ciphers
- RC4, RC5, RC6
- Weaknesses

Asymmetric Encryption

- Public-key cryptography principles and operation
- RSA
- Diffie-Hellman Key Exchange
- Elliptic Curve Cryptography

Cryptographic data integrity algorithms

- Cryptographic hash functions
- MD5, SHA, RIPEMD
- Message authentication codes
- Weaknesses
- Digital signatures

Key management and distribution

- Symmetric key distribution using symmetric encryption
- Symmetric key distribution using asymmetric encryption
- Distribution of public keys
- X.509 Certificates
- Public Key Infrastructure (PKI)

Attacks

- Ciphertext-only
- Known plaintext
- Chosen plaintext
- Chosen ciphertext
- Birthday paradox
- Man-in-the-middle

Applications

- Random number generators
- SSL/TLS protocol

	<ul style="list-style-type: none"> - Virtual Private Networks (VPN) - Steganography - Cryptography and malware - Cryptography and the cloud - Cryptocurrency - Digital rights management (DRM) 																		
Teaching Methodology	<p>The theoretical material will be delivered during the lectures. The students are expected to actively participate and prepare for workshops, assessment briefs and other matters relating to cryptography. During the workshops, students will be introduced to cryptographic concepts, tools and techniques, and have the opportunity to participate in hands-on activities. Synchronous (i.e. in class) and/or asynchronous (i.e. blogs) discussions will take place to further discuss practical findings. As a result of the discussions, additional directed reading may be required. Speakers from leading security organizations will be invited, where possible, to deliver live invited talks and enhance the students' experience.</p>																		
Bibliography	<p>Online Reading List:</p> <ol style="list-style-type: none"> 1. Cryptography and Network Security: Principles and Practice 7th Edition, 2021, William Stallings, ISBN-13: 978-0134444284, ISBN-10: 0134444280 2. Modern Cryptography: Applied Mathematics for Encryption and Information Security, 1st Edition, William Easttom, 2021, ISBN-13: 978-3030631147, ISBN-10: 3030631141 																		
Assessment	<p>The method of assessment for this module has been designed to test all the learning outcomes. Students must demonstrate successful achievement of these learning outcomes to pass the module.</p>																		
	<table border="1"> <thead> <tr> <th>Number of Assessments</th> <th>Form of Assessment</th> <th>% weighting</th> <th>Size of Assessment /Duration/ Wordcount (indicative only)</th> <th>Category of assessment <i>(select 1 of written exam/practical assessment/course work –see guidance notes)</i></th> <th>Learning Outcomes being assessed</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Report including results of an investigation and personal reflection</td> <td>50%</td> <td>2000 word report</td> <td>Coursework</td> <td>2,3,4</td> </tr> <tr> <td>1</td> <td>Examination</td> <td>50%</td> <td>2 hours</td> <td>Written exam</td> <td>1,2,3</td> </tr> </tbody> </table>	Number of Assessments	Form of Assessment	% weighting	Size of Assessment /Duration/ Wordcount (indicative only)	Category of assessment <i>(select 1 of written exam/practical assessment/course work –see guidance notes)</i>	Learning Outcomes being assessed	1	Report including results of an investigation and personal reflection	50%	2000 word report	Coursework	2,3,4	1	Examination	50%	2 hours	Written exam	1,2,3
	Number of Assessments	Form of Assessment	% weighting	Size of Assessment /Duration/ Wordcount (indicative only)	Category of assessment <i>(select 1 of written exam/practical assessment/course work –see guidance notes)</i>	Learning Outcomes being assessed													
1	Report including results of an investigation and personal reflection	50%	2000 word report	Coursework	2,3,4														
1	Examination	50%	2 hours	Written exam	1,2,3														
<p>For successful completion of this module a minimum aggregate mark of 50% must be achieved.</p>																			
Language	English																		

