جامعة أم القيوين
Umm Al Quwain University

College of Arts & Sciences

Program Name اسم البرنامج	**Bachelor of Science in Cybersecurity**
Program Code/Number رمز ورقم البرنامج	
Major CIP	11.1003
Authoring team. فريق عمل إعداد البرنامج	- Dr. Saada Khadragy - Dr. Ali Siam
Date of publication تاريخ الإصدار	7 June 2024
Initial Accreditation Date تاريخ الاعتماد الأولي للبرنامج	
Last Renewal of Accreditation Date تاريخ تجديد اعتماد البرنامج	-
Next reaccreditation due date تاريخ استحقاق إعادة الاعتماد التالي	
International Accreditation Date تاريخ الاعتماد الدولي	-
Last update أخر تحديث	30 December 2025

Table of Contents

Introduction 4
Teaching and Learning Methodologies 4
Program Objectives 5
Program Learning Outcomes 6
The program completion requirements 6
Program Structure 7
The University Requirements: ..... **Error! Bookmark not defined.**
General Education 7
General Electives 8
Degree Requirements 8
Major Requirements 9
Major Electives 9
Internship 10
Student Support Services 10
General Admission Requirements 11
Facilities 12
Teaching and Program Quality Enhancement 12
Student Feedback on the Course and Instructor 13
Teaching Report 13
Course File Report 13
Faculty Performance Evaluation 13
Advisory Board 14
Quality Assurance Indicators 14
Learning Management Systems 15
Grading Rubrics 15
Moderation of Final Exams 15
Measurement of PLO - CLO Achievement 15
Faculty Research Support 15
Academic Advising and Office Hours 15
Alumni Survey 15
Program Matrix 16
Program Compulsory courses and PLOs Matrix 16

Program Free Elective courses and PLOs Matrix 17

Program Compulsory General Education courses and PLOs Matrix 18

Program Free Elective General Education courses and PLOs Matrix 18

Appropriate Program learning outcomes with the output of the Emirates Qualifications Framework 20

Appropriate PLOs and QFE (Knowledge): 20

Appropriate PLOs and QFE (Skills): 22

Appropriate PLOs and QFE (Responsibility): 23

Introduction:

The Cybersecurity program is one of the programs offered by the College of Arts and Sciences at Umm Al Quwain University. The University of Umm Al Quwain (UAQU) aspires to be one of the reputable institutions of higher education in the UAE and regionally known for excellence and innovation in teaching and learning, research, and community engagement. UAQU will achieve this by engaging effectively with the community, establishing links with industry and other global universities and institutions, and adopting international best practices and innovation in teaching, research, and scholarship. UAQU is dedicated to significantly contribute to the socio-cultural and economic growth of the UAE and the region.

The BS in Cybersecurity program will provide the students with the professional competence and breadth of knowledge in the field of cybersecurity which includes information and network security. Students enrolled in this program will gain both management skills and the technical knowledge which are needed to plan, acquire, operate, manage, and evaluate an organization's information security operations. The ultimate goal of this program is to build industry-standard secure systems, applications and networks based on proven and innovative practices.

Teaching and Learning Methodologies

The Cybersecurity program faculty members, through the college/Program Committees, make sure that the instructors do cover the course material on time as specified in the course syllabus which contains a full description of the learning outcomes and course objectives. It also contains a week-by-week study schedule; assessment methods to be used, IT tools used (where applicable); online resources (web, Moodle, reference links, among others), and university policies regarding attendance, cheating and plagiarism.

Teaching and learning methodologies in a Bachelor in Cybersecurity program emphasize a blend of theoretical knowledge and practical skills. Instruction often includes traditional lectures to cover fundamental concepts such as cryptography, network security, and ethical hacking. However, to ensure students gain hands-on experience, many programs incorporate lab-based sessions and simulations where students can engage in real-world scenarios such as penetration testing and incident response. Collaborative projects and problem-based learning are commonly used to foster teamwork and critical thinking. Additionally, the integration of online resources and virtual labs allows for flexible, self-paced learning. Internships and industry partnerships further enhance the curriculum, providing students with exposure to current cybersecurity

challenges and practices. This multifaceted approach equips graduates with the technical proficiency and strategic understanding necessary to navigate the dynamic field of cybersecurity.

The faculty members teach the various courses of the program, each according to his/her specialization, and their academic ranks range from professor, associate professor, and assistant professor. Also, teaching assistants (if required) who can be used in the practical parts. The student registers at least 12 credit hours (4 courses) per semester, and a maximum of 18 credit hours (6 courses).

Students are assessed on course work that includes term tests and final examinations, in and outside class assigned work (e.g., class presentations of projects, case studies, written home assignments, in class quizzes, etc.), and class participation (when required).

Attendance is compulsory and is regulated by an Attendance Policy which is published in the policies and procedures.

Program Objectives

- Establishing clear and direct objectives for the program is essential for its success, particularly in the context of ongoing evaluation efforts and periodic reviews to assess goal attainment. The following are the program's goals, anticipated to be achieved during study. Examining emerging technologies from a scientific perspective enables students to understand the issues and challenges facing their communities and to contribute effectively to developing appropriate solutions. This approach underscores a commitment to maintaining and promoting national identity.

  PO1: To provide students with a strong foundation in computing principles and other relevant disciplines necessary to analyze complex computing problems and identify solutions.

  PO2: To equip students with the knowledge and skills to design, implement, and evaluate secure computing-based solutions that meet specified requirements.

  PO3: To develop students' ability to communicate effectively in a variety of professional contexts, including technical reports, presentations, and teamwork.

  PO4: To instill in students an understanding of the legal and ethical principles that govern computing practice and to prepare them to make informed judgments based on these principles.

PO5: To foster in students the ability to function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

PO6: To provide students with the knowledge and skills to apply security principles and practices to maintain operations in the presence of risks and threats.

Program Learning Outcomes

- The BSCS program adheres to the QF Emirates Level 7 descriptors. The learning outcomes for the courses are also designed to meet the QF Emirates requirements.
  The student outcomes of the Cybersecurity program map directly onto the ABET cybersecurity and similarly named computing programs Criterion (1) - (6).

Upon successful completion of this program, students will be able to:

1. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. (PLO1)

2. Design computing-based solutions that address security requirements while considering sustainable practices. (PLO2)

3. Communicate effectively in a variety of professional contexts. (PLO3)

4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. (PLO4)

5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (PLO5)

6. Apply security principles and practices to maintain operations in the presence of risks and threats. (PLO6)

The program completion requirements

The Bachelor of Science in Cybersecurity provides a sequence of courses that have university requirements and major courses. A student who can complete a bachelor's degree program at UAQU, must meet the following criteria:

- Graduation requirements include the successful completion of 43 courses (120 credit hours: 66 compulsory credit hours for the major, and 9 Free Elective credit hours for the major, and 18 credit hours for degree requirements, in addition to 27 credit hours for GED (24 compulsory and 3 electives).

Program Structure

Course Type	Courses	Credit
General Education	9	27
Degree Requirements	6	18
Major Requirements	22	59
Major Electives	3	9
Internships	2	4
Senior Graduation Project	1	3
Total	43	120

General Education

No.	Course Code	Description	Prerequisite(s)	Cr.H
1	ENG103	English I	-	3
2	ENG104	English II	ENG103	3
3	MTH100	College Algebra	-	3
4	CIT100	Computer Concepts and Applications	-	3
5	GED101	Islamic Culture	-	3
6	GED112	Contemporary Emirati Studies	-	3
7	IES111	Innovation, Entrepreneurship, and Sustainability	-	3
8	IES112	Introduction to Environmental Sustainability	-	3
Total				24

General Electives

No.	Course Code	Elective courses	Prerequisite(s)	Cr.H
1	GED130	Introduction to GIS	-	3
2	GED140	Conceptual Physics	-	3
3	GED150	Critical Thinking	-	3
4	GED160	Psychology in Everyday Life	-	3
5	GED162	Corporate Social Responsibility	-	3
6	GED180	Human Behavior and Socialization	-	3
Total (ONLY one course)				3

The degree requirements:

Degree Requirements

No.	Course Code	Course Title	Prerequisite(s)	Cr.H
1	MAT110	Calculus I	MTH 100	3
2	MAT120	Calculus II	MAT110	3
3	MAT130	Linear Algebra	MTH100	3
4	MAT140	Probability and Statistics	-	3
5	MAT150	Numerical Analysis	MAT110	3
6	MAT160	Discrete Mathematics	MTH100	3
Total				18

Major Requirements

No.	Course Code	Major Courses - Titles	Prerequisite(s)	Cr.H
1	SYS100	Computer Programming	CIT100	3
2	SYS240	Introduction to Cyber Security Engineering	CIT100	3
3	SYS310	Object Oriented Programming	SYS100 Co-requisites	3
4	SYS320	Object Oriented Programming Lab		1
5	SYS330	Operating Systems	CIT100, SYS100	3
6	SYS340	Data Structures	SYS100	3
7	ECE210	Digital Systems	- Co-requisites	3
8	ECE325	Digital Systems Lab		1
9	SYS345	Fundamentals of Data & Network Communication for Cybersecurity	CIT100, ECE210	3
10	SYS350	Introduction to Network Security	SYS345	3
11	SYS370	Database Management Systems	SYS340, SYS100	3
12	SYS385	Cybersecurity Architecture and Design	SYS240	3
13	SYS410	Cryptography Fundamentals	MAT150	3
14	SYS425	Secure Software Engineering	SYS240	3
15	SYS428	Information Security Policy and Governance	SYS340	3
16	SYS430	System Security and Resilience	SYS240	3
17	SYS440	Ethical Hacking Laboratory	SYS350	2
18	SYS450	Penetration Testing Laboratory	SYS350, SYS370	2
19	SYS460	Computer Forensics Laboratory	SYS350, SYS370	2
20	SYS470	Industrial Control Systems Security	SYS430	3
21	SYS472	Information Privacy and Security	SYS385	3
22	SYS474	Reverse Software Engineering	SYS100	3
23	SYS490	Senior Graduation Project	SYS486 + 90 cr. Hrs	3
Total				62

Major Electives

No.	Course Code	Elective courses	Prerequisite(s)	Cr.H
1	SYS476	Cyber Physical Systems	80 cr. Hrs	3
2	SYS478	Special topics in Cybersecurity	80 cr. Hrs	3

3	SYS480	Methods of User Authentication	80 cr. Hrs	3
4	SYS482	Intrusion Detection	80 cr. Hrs	3
Total (ONLY three courses)				9

Internship

No.	Course Code	Description	Prerequisite(s)	Cr.H
1	SYS485	Internship I	60 cr. Hrs	2
2	SYS486	Internship II	SYS485 + 80 cr. Hrs	2
Total				4

Student Support Services

The Student Service Services (SSS) is a team comprises of an SSS Head and staff members. The staff members report to the SSS Head. SSS is the central point for information and advice for all students, not just those overseas students. The SSS provides a wide range of services and will assist students with the following:

- Registration
- Immigration
- Information
- Examinations
- Certificates
- ID Cards
- Academic Counselling
- Personal Counselling
- Complaints & Suggestions
- Students Clubs & Organization
- Personal Development Planning (PDP)

- Transcript
- Fee Payment
- Application to Full-Time Program

UAQU seeks to achieve its mission, as the student is the main pillar upon which the philosophy of UAQU is based and is the focus of the educational process. The implementation of the extra-curricular activities, where SSS are carried out in cooperation with the colleges and academic programs is mainly to achieve excellence for the student.

On the other hand, UAQU has a scholarship system that will be applied accordingly to students expected to join the Cybersecurity program, as UAQU firmly believes that supporting distinguished students is an important key to develop their distinction and encouraging them to

General Admission Requirements

Every applicant is required to submit the following documents:

- Completion of UAE's High Secondary School Certificate, or its equivalent, with a minimum score of 70%.
- Proof of English language proficiency through one of the following certificates:
  - IELTS: minimum score of 5
  - TOEFL ITP: minimum score of 500
  - TOEFL iBT: minimum score of 61
  - TOEFL CBT: minimum score of 173
  - Linguaskill: minimum level B2
  - Any other English proficiency test approved by the Commission for Academic Accreditation (CAA).
- Proof of mathematics proficiency through the SAT, with a minimum score of 450.
- Passing a personal/skills interview set by the committee.
- Any other requirements requested by the University in accordance with UAQU policies and procedures.

Exemption from English Language Proficiency Requirement:

Students applying to the program may be exempted from the English proficiency requirement in the following cases:

- Passing the Umm Al Quwain University English placement test with a minimum score of 80.
- Or obtaining a score of 80 or higher in English in the secondary school certificate.
- Or achieving an overall secondary school average of 80 or above.
- Or exemption for students who studied non-Ministry of Education curricula, provided that the curriculum is delivered in English.

Exemption from Mathematics Proficiency Requirement:

Students applying to the program may be exempted from the mathematics proficiency requirement in the following cases:

- Passing the Umm Al Quwain University mathematics placement test with a minimum score of 75.
- Or obtaining a score of 80 or higher in mathematics in the secondary school certificate.
- Or achieving an overall secondary school average of 80 or above.

Facilities

The University aims to create an environment in which education of the highest quality can be undertaken. This includes:

- appropriate physical facilities (e.g. laboratories, libraries, archives, offices, equipment, IT systems) and professional support for teaching activities.
- an intellectual environment conducive to unfettered enquiry which allows interactions among students.
- The library provides resources and services to its faculty, students, staff and the community through a central facility located in the University campus. The Library is open every weekday except Saturdays, Sundays if required based on the class schedule. Working hours are Monday-Friday from 8:00 a.m. to 06:00 pm. The Library extends its services until late in the evening on special days to serve evening classes *(if any)*.
- The library's collections shall comprise all types of recorded information, including print materials in all formats, audio-visual materials, sound recordings, materials used with computers graphics, and three-dimensional materials;

Teaching and Program Quality Enhancement

The College undertakes continuous, integrated, and institution-wide research-based planning and evaluation processes. These processes encompass systematic program reviews that drive ongoing enhancements and substantiate the program's effective fulfillment of its mission. Comprehensive documentation of data collected through consistent and rigorous assessment informs decision-making and provides concrete evidence of the College's unwavering commitment to continuous improvement.

The College prioritizes data collection, analysis, and reporting on program outcomes. It gathers data from students, alumni, and faculty members to evaluate program

performance and guide planning aligned with the College's strategic objectives. The sources of collected data include:

Student Feedback on the Course and Instructor:

Students' Feedback on the course and instructor, which is conducted at the end of each semester, provides feedback on course instructions, course delivery, assessment methods, relevance of topics, usage of learning resources, feedback on quality of teaching, approach to students, response to student's queries and related teaching learning aspects. The analysis results and recommendations of the students' feedback are sent to the faculty for their comments, action plan and improvement of the accepted recommendations.

Teaching Report:

To review and ensure the level of implementation of the course syllabus, the faculty should submit teaching report in the seventh week (before midterm exam) and the final teaching report in 14th week (before the final exam). The report is reviewed and discussed with the faculty by the head of the department for further development in class management for the current and coming semesters.

Course File Report:

Course file report is prepared by the instructor on completion of the course. The report provides a comprehensive instructor review of the implementation of the course, achievement level of CLOs, the challenges faced by the instructor and corrective actions required for implementation from the coming semester in addition to the follow up process to ensure the implementation of the action plan.

Faculty Performance Evaluation:

Faculty performance evaluation, a comprehensive self-evaluation of faculty performance shall be submitted at the end of the academic year. Faculty performance for the year is evaluated on teaching, research and publications, involvement in college development, community services and student advising services. Self –evaluation provides faculty with an understanding about his / her performance during the year and improvement needed during the next academic year. This helps the faculty to identify the areas of improvement. Continuous self-evaluation supports to maintain quality in teaching-learning process, other academic and extracurricular activities.

Advisory Board:

The aim of establishing the advisory board is to review the various curricula and extracurricular activities to support the objectives of the program, including the educational curriculum and the student's research activities.

The advisory board aims to enhance and maintain the competitive advantage of Umm Al Quwain University in academic activities. This advisory board includes a selection of specialists from related organizations in the society as well as academic specialists, related to the specialization to enhance the efficiency and effectiveness of all academic activities in the program. The main tasks will be as follows:

- Assessing, evaluating and planning all existing academic activities.
- Developing recommendations aimed at continuous improvement and quality.
- Ensure that the program learning outcomes are in accordance with the requirements of the labor market from this program.

Quality Assurance Indicators

The college aims to engage in a systematic and broad-based planning and assessment process which demonstrates that the program is effectively accomplishing its mission. The goal of continuous improvement is to meet the highest standards of quality and excellence of the program for higher levels of student learning.

The college identifies the expected outcomes of its educational program and provides evidence of improvement based on analysis of those results. To assure the quality enhancement, the college uses a variety of assessment methods, and demonstrates the use of results for the improvement of the academic program.

Based on the student feedback, faculty evaluation, course review reports and teaching reports, the areas of improvement in teaching effectiveness can be identified, and reported to respective faculty members. Measures are taken for the proper implementation of recommendations from the feedback. This process is approved and implemented at the college level as part of the improvement to the quality of academic programs, which is monitored by the IE department and Head of department.

To improve the quality of the program teaching effectiveness, the college implements the following actions:

Learning Management Systems

Through the Implementation of eLearning Management Systems (LMS), effective control and coordination could be created for class management for all subjects offered at the college. In addition, the college implements a Plagiarism detection software which is linked to the LMS aiming to review the students' submissions. This enhances students' capability for independent/group thinking and in submitting their high-quality work.

Grading Rubrics

Grading rubrics are implemented for all formative and summative assessment of course work. This enhances teaching effectiveness in proper delivery of the course through proper evaluation of both formative and summative assessments.

Moderation of Final Exams

Final Exam Questions Paper and modal Answers, are moderated by the college before the exams. This helps to standardize question papers and improve the examinations quality, as well as to observe that the course delivery meets the expected level and has covered the CLOs.

Measurement of PLO - CLO Achievement

CLOs achievement is measured from the Course Learning Outcome Assessment Mapping. In case in failure in achieving the learning outcomes, that shall be discussed with the faculty. Matrics contains, the matrix of PLO – CLO achievement, review of program effectiveness, and action plan for further improvement in course delivery.

Faculty Research Support

The college considers academic-research as a vital tool for quality improvement in teaching. The college urges faculty members to publish in listed and indexed journals. In addition, the college encourages faculty research, by providing annual research excellence awards.

Academic Advising and Office Hours

Office hours are allocated for faculty members to follow up with the students and provide the proper academic advice regarding choosing the subjects to be enrolled or any other related to their study. This enables advisors to provide the academic advising to the students, and other administrative and academic activities.

Alumni Survey

The college regularly conducts alumni survey for every academic year. The results shall be collected and discussed to be raised for the necessary action(s).

Program Matrix

Program Compulsory courses and PLOs Matrix

Program Learning Outcomes		**A 1**	**A 2**	**A 3**	**B 1**	**B 2**	**B 3**	**C1**	**C2**	**C3**
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
SYS100	Computer Programming	√	√	√	√		√	√	√	√
SYS240	Introduction to Cyber Security Engineering	√	√	√	√	√		√	√	√
SYS310	Object-Oriented Programming	√	√	√	√	√		√	√	
SYS320	Object-Oriented Programming Lab	√	√	√	√		√	√		√
SYS345	Fundamentals of Data & Network Communication for Cybersecurity	✓			✓	✓	✓	✓	✓	✓
SYS330	Operating Systems and Lab	√			√		√	√		√
SYS340	Data Structures	√	√		√			√	√	√
ECE210	Digital Systems	✓	✓		✓	✓	✓	✓		✓
ECE325	Digital Systems Lab				✓	✓	✓	✓	✓	✓
SYS350	Introduction to Network Security	√	√	√		√	√	√	√	√
SYS370	Database Management Systems	√	√	√	√	√	√	√		√
SYS410	Cryptography Fundamentals	√	√		√	√	√	√		√
SYS425	Secure Software Engineering	√	√	√	√			√		√
SYS428	Information Security Policy and Governance	√	√	√			√	√		√
SYS430	System Security and Resilience		√	√			√	√	√	√
SYS440	Ethical Hacking laboratory	√	√	√	√		√	√		
SYS450	Penetration Testing laboratory			√	√	√		√	√	

Program Learning Outcomes		A 1	A 2	A 3	B 1	B 2	B 3	C1	C2	C3
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
SYS460	Computer Forensics laboratory	√	√	√		√	√		√	
SYS470	Industrial Control Systems Security		√		√			√		√
SYS472	Information Privacy and Security			√				√		√
SYS474	Reverse Software Engineering	√	√	√	√	√	√	√	√	√
SYS 485	Internship I	√		√	√		√	√	√	√
SYS 486	Internship II			√		√	√	√		√
SYS490	Senior Graduation Project			√		√	√	√	√	√

Program Free Elective courses and PLOs Matrix

Program Learning Outcomes		A 1	A 2	A 3	B 1	B 2	B 3	C1	C2	C3
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
SYS476	Cyber Physical Systems	√	√	√			√	√		√
SYS478	Special topics in Cybersecurity	√		√			√	√		√
SYS480	Methods of User Authentication				√		√	√		√
SYS482	Intrusion Detection	√		√	√			√	√	√

Program Degree Requirements courses and PLOs Matrix

Program Learning Outcomes		A 1	A 2	A 3	B 1	B 2	B 3	C1	C2	C3
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
MAT 110	Calculus I	✓	✓		✓			✓		
MAT 120	Calculus II		✓		✓			✓		

MAT 130	Linear Algebra	✓		✓		✓			✓	
MAT 140	Probability and Statistics		✓		✓				✓	
MAT 150	Numerical Analysis	✓				✓		✓		
MAT 160	Discrete Mathematics		✓		✓				✓	✓

Program Compulsory General Education courses and PLOs Matrix

Program Learning Outcomes		**A 1**	**A 2**	**A 3**	**B 1**	**B 2**	**B 3**	**C1**	**C2**	**C3**
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
ENG 103	English I		√			√		√	√	
ENG 104	English II		√			√		√	√	
CIT 100	Computer Concepts and Applications		√		√			√		√
GED 101	Islamic Culture	√	√			√		√		
GED 110	UAE Society	√	√		√	√		√		
GED 112	Contemporary Emirati Studies		√		√					
IES 111	Innovation, Entrepreneurship, and Sustainability		√					√		
IES 112	Introduction to Environmental Sustainability		√			√		√		
MTH 100	College Algebra							√	√	

Program Free Elective General Education courses and PLOs Matrix

Program Learning Outcomes		**A 1**	**A 2**	**A 3**	**B 1**	**B 2**	**B 3**	**C1**	**C2**	**C3**
Course Code	**Course Title**	**Knowledge**			**Skills**			**Responsibility**		
GED 130	Introduction to GIS	√			√	√		√		
GED 140	Conceptual Physics	√			√			√		

GED 150	Critical Thinking	√	√		√	√		√		
GED 160	Psychology in Everyday Life	√	√		√		√	√		
GED 162	Corporate Social Responsibility	√	√				√			
GED 180	Human Behavior and Socialization	√	√			√		√		

Appropriate Program learning outcomes with the output of the Emirates Qualifications Framework in the Bachelor degree level (level 7)

Appropriate PLOs and QFE (Knowledge):

1. analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. (PLO1)

2. Design computing-based solutions that address security requirements while considering sustainable practices. (PLO2)

3. Communicate effectively in a variety of professional contexts. (PLO3)

4. Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. (PLO4)

5. Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (PLO5)

6. Apply security principles and practices to maintain operations in the presence of risks and threats. (PLO6)

QFE	Cybersecurity program learning outcomes		
Knowledge	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions	Design computing-based solutions that address security requirements while considering sustainable practices..	Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
Specialized factual and theoretical knowledge and an understanding of the boundaries in a field of work or discipline, encompassing a broad and coherent body of knowledge and concepts, with substantive depth in the underlying principles and theoretical concepts	SYS100 SYS240 SYS310	SYS320 SYS330 SYS340	SYS350 SYS370
QFE	Cybersecurity program learning outcomes		

Knowledge	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	Design computing-based solutions that address security requirements while considering sustainable practices..
An understanding of allied knowledge and theories in related fields of work or disciplines and in the case of professional disciplines including related regulations, standards, codes, conventions	SYS410 SYS425	SYS428 SYS430	SY440 SY460
Understanding of critical approach to the creation and compilation of a systematic and coherent body of knowledge and concepts gained from a range of sources	SYS470 SYS472	SYS470 SYS472	SYS478 SYS478

Appropriate PLOs and QFE (Skills):

QFE	Cybersecurity Program Learning Outcomes		
Skills	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline	Apply security principles and practices to maintain operations in the presence of risks and threats.	Design computing-based solutions that address security requirements while considering sustainable practices..
Technical, creative and analytical skills appropriate to solving specialized problems using evidentiary and procedural based processes in predictable and new contexts that include devising and sustaining arguments associated with a field of work or discipline	SYS480 SYS482	SYS 485 SYS 486	SYS490 SYS478 SYS100
Evaluating, selecting and applying appropriate methods, procedures or techniques in processes of investigation towards identified solutions	SYS478 SYS 485	SYS490 SYS478 SYS 486	SYS480 SYS482 SYS478
Evaluating and implementing appropriate research tools and strategies associated with the field of work or discipline	SYS470 SYS472	SYS100 SYS240 SYS310	SYS482 SYS478
Highly developed advanced communication and information technology skills to present, explain and/or critique complex and unpredictable matters	SYS428 SYS430	SYS320 SYS330 SYS340	SYS320 SYS240 SYS310

Appropriate PLOs and QFE (Responsibility):

QFE	Cybersecurity Program Learning Outcomes					
Responsibility	Communicate effectively in a variety of professional contexts.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Design computing-based solutions that address security requirements while considering sustainable practices.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
Can take responsibility for developing innovative and advanced approaches to evaluating and managing complex and unpredictable work procedures and processes, resources or learning	SYS 485 SYS 486 SYS490	SYS476 SYS478 SYS480	SYS482 SYS 485	SYS370 SYS410	SY470 SYS472 SYS474	SYS430 SYS440 SYS460
Can manage technical, supervisory or design processes in unpredictable, unfamiliar and varying contexts	SYS480 SYS482	SYS470 SYS472 SYS474	SYS476 SYS478	SYS478 SYS340	SYS240 SYS 485	SYS320 SYS330
Can express an internalized, personal view,	SYS425	SYS 486	SYS478	SYS 486	SYS470	SYS320

QFE	Cybersecurity Program Learning Outcomes					
Responsibility	Communicate effectively in a variety of professional contexts.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Design computing-based solutions that address security requirements while considering sustainable practices.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
and accept responsibility to society at large and to socio-cultural norms and relationships	SYS428	SYS490	SYS478 SYS480	SYS490	SYS474	SYS474 SYS478
Can participate in peer relationships with qualified practitioners and lead multiple, complex groups	SYS480 SYS482 SYS478	SYS100 SYS240	SYS340 SYS370	SYS310 SYS330	SYS350 SYS320	SYS460 SYS482 SYS 485
Can function with full autonomy in technical and Supervisory contexts and adopt para-professional roles with little guidance	SYS480 SYS240 SYS478	SYS478 SYS480 SYS370	SYS474 SYS478	SYS460 SYS482 SYS 485	SYS476 SYS478	SYS480 SYS320
Can take responsibility for managing the professional development and direct	SYS410 SYS425	SYS430 SYS440	SYS474 SYS478	SYS430 SYS440	SYS476 SYS478	SYS100 SYS240

QFE	Cybersecurity Program Learning Outcomes					
Responsibility	Communicate effectively in a variety of professional contexts.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Design computing-based solutions that address security requirements while considering sustainable practices.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
mentoring of individuals and groups	SYS428	SYS460	SYS320 SYS430 SYS440 SYS310 SYS330	SYS310 SYS330	SYS478 SYS480 SYS482 SYS 485	SYS310 SYS320 SYS330 SYS340
Can self-evaluate and take responsibility for contributing to professional practice, and undertake regular professional development and/ or further learning can manage learning	SYS100 SYS240	SYS100 SYS240 SYS470 SYS474	SYS100 SYS240	SYS480 SYS240 SYS478	SYS478 SYS478 SYS480	SYS470 SYS472 SYS474

QFE	Cybersecurity Program Learning Outcomes					
Responsibility	Communicate effectively in a variety of professional contexts.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Design computing-based solutions that address security requirements while considering sustainable practices.	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.	Apply security principles and practices to maintain operations in the presence of risks and threats.	Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
Can contribute to and observe ethical standard	SYS310 SYS320	SYS478 SYS480 SYS370	SYS340 SYS350 SYS370	SYS310 SYS320	SYS340 SYS370	SYS 486 SYS490