



University of Prince Mugrin
College of Computer and Cyber Sciences

Program Handbook

Cyber Security and Forensic Computing (CSFC)

Department Of Cyber Security and Forensic Computing

May 2024

Cyber Security and Forensic Computing (CSFC)

Program Handbook V3.0

Bachelor's Degree Program

College of Computer and Cyber Sciences

University of Prince Mugrin

“

At UPM, we are committed to providing excellent education and research in computer science, aiming to address the needs of our communities and contribute to economic growth. As technology rapidly evolves, the need for skilled cybersecurity professionals becomes even more critical

”

Dr. Ahmed Showail

Dean of the College of Computer and Cyber Sciences

“

The Cyber Security and Forensic Computing department has a full focus on achieving its mission. This mission centers on producing motivated graduates who not only possess vital knowledge and skills, but also deeply passionate about the cyber security field. We prepare our student to be leaders in their field and enablers of a safe society.

”

Dr. Khaled Khankan

Head of the Cyber Security and Forensic Computing Department

Table of Content

1. Introduction	7
1.1. Background and Motivation	7
2. Program Details	8
2.1. Mission	8
2.2. Objectives	8
2.3. Duration	9
2.4. Unique features	9
2.5. Student outcomes	10
3. Admission Requirements	11
3.1. High School Certificate or Equivalent	11
3.2. Recent High School Certificate	11
3.3. Qiyas Test Grades	11
3.4. Good Conduct	11
3.5. Academic and Disciplinary Record	11
3.6. Medical Fitness	11
3.7. Placement Test	12
3.8. Enrollment in Preparatory Year	12
4. Graduation Requirements	13
4.1. Foundational Courses	13
4.2. Core Courses	14
4.3. Elective Courses	15
4.4. Minimum GPA	15
4.5. Total Credits	16
4.6. Grading System	16
5. Course Descriptions	18
5.1. First Level (Total Credits:17)	18
5.2. Second Level (Total Credits 18)	21
5.3. Third Level (Total Credits 18)	24
5.4. Fourth Level (Total Credits: 15)	26
5.5. Fifth Level (Total Credits: 18)	28
5.6. Sixth Level (Total Credits: 17)	31
5.7. Summer (Total Credits: 1)	33
5.8. Seventh Level (Total Credits: 16)	34

5.9. Eight Level (Total Credits: 12)	36
5.10. Elective Courses	38
6. Advising and Support Services	43
6.1. Academic Advising	43
6.2. Faculty Office Hours	43
6.3. Resources for Success	43
6.4. English Language Support Center	44
6.5. Arabic Language Support Center	44
6.6. Counseling Center	44
6.7. Scholarship Unit	45
7. Policies and Procedures	47
8. Student Resources	49
8.1. Library	49
8.2. Computer Labs	49
8.3. Research Centers	49
8.4. Student Organizations Related to Cybersecurity	49
8.5. Transportation Services	50
9. Internship and Career Opportunities	51
9.1. Finding Internships and Co-op Opportunities	51
9.2. Career Placement Services	51
9.3. Industry Certifications	51
10. Appendices	52
10.1. Sample Degree Plans	53
10.2. Faculty Contact Information	55

1. Introduction

1.1. Background and Motivation

In recent years, the field of computer science has undergone rapid expansion, with a particular emphasis on areas such as communications technology, electronics, software, and the Internet. This growth is reflected in the increasing number of Internet users in the Kingdom of Saudi Arabia, which has reached a significant 14.7 million, constituting 54% of the population. Recognizing the importance of meeting the evolving needs of customers and users, as well as developing essential services, Saudi specialists have been called upon to demonstrate expertise across various domains within computer science. To address these demands, the Faculty of Computer has taken proactive steps to provide specialized programs that equip students with both theoretical knowledge and practical skills, ensuring they are well-prepared for careers in the field.

Notably, the College of Computer and Cyber Sciences has introduced a program on Cyber Security and Forensic Computing, recognizing the unique challenges posed by cyber threats in the region. With Saudi Arabia being a repeated target for hackers and electronic warfare leaders in the Middle East, the imperative for security information experts to safeguard the e-Kingdom's security cannot be overstated. In this dynamic landscape, where cyber threats continue to evolve, cyber security emerges as a critical priority, requiring constant vigilance and continuous efforts to enhance protection, detection, and mitigation capabilities. This program sets the stage for a deeper exploration of the importance of cyber security education in addressing the pressing security challenges faced by the Kingdom.

We are excited to welcome you to this program and empower you to become a leader in the field of cybersecurity!

2. Program Details

The Bachelor's Degree in Cyber Security and Forensic Computing is a comprehensive four-year program designed to equip students with the knowledge, skills, and expertise necessary to navigate the complex landscape of cybersecurity threats and defenses. Throughout the program, students engage in a rigorous curriculum that integrates theory with practical applications, preparing them for careers in cybersecurity across various sectors. Below is an overview of the program, including its mission, objectives, duration, unique features and learning outcomes:

2.1. Mission

The mission of our program is to contribute to societal security by graduating motivated and passionate cyber security professionals who possess the vital practical skills and theoretical knowledge and by engaging in multidisciplinary research.

2.2. Objectives

Derived from the mission, the CSFC program defined its targeted Program Educational Objectives listed in the table below:

CSFC Program Educational Objectives (PEOs)		
PEO-1	Professional Development	CSFC graduates take practical and concrete initiatives to acquire cyber security and forensics education and continuously grow as professionals ever-focused on improving their skillset and competencies
PEO-2	Social Contribution	CSFC graduates draw on the versatility of their experiences to contribute positively, ethically and respectfully, to the world around them, using their cyber security skillset only as a force for good
PEO-3	Research-Based Approach	CSFC graduates use their highly developed skills in research and enquiry to identify and creatively tackle real-world problems
PEO-4	Practical Problem Solvers	CSFC graduates take a hands-on approach to problem solving by utilizing the practical and theoretical skillset they have acquired over the course of their education
PEO-5	Committed Team Players	CSFC graduates build strong professional relationships and work efficiently with others to achieve a common goal

2.3. Duration

The Bachelor's Degree in Cyber Security and Forensic Computing program is structured as a four-year program, typically spanning eight levels. This duration allows students to delve deeply into the core concepts of cybersecurity while also providing opportunities for specialization and hands-on experience.

2.4. Unique features

1. **Specialized Concentrations:** The program offers a range of specialized concentrations or tracks that allow students to tailor their education to their specific interests and career goals. These concentrations include areas such as:
 - a. Cyber Defense and Operations
 - b. Digital Forensics and Incident Response
 - c. Cybersecurity Policy and Governance
 - d. Network Security and Penetration Testing
 - e. Secure Software Development
2. **Interdisciplinary Approach:** Students benefit from an interdisciplinary approach to cybersecurity education, drawing from diverse fields such as computer science, information technology, mathematics, and humanities. This holistic perspective enables students to understand cybersecurity challenges from multiple angles and develop comprehensive solutions.
3. **Hands-On Learning:** The program emphasizes hands-on learning experiences, providing students with opportunities to apply theoretical knowledge in real-world scenarios. Through laboratory exercises, simulations, internships, and capstone projects, students gain practical skills and insights that are invaluable in the cybersecurity profession.
4. **Industry Partnerships:** The program cultivates strong partnerships with industry leaders, cybersecurity firms, government agencies, and research institutions. These partnerships offer students access to internships, guest lectures, networking opportunities, and mentorship programs, enhancing their professional development and preparing them for success in the field.
5. **Cutting-Edge Curriculum:** The curriculum is continuously updated to reflect the latest advancements, trends, and best practices in cybersecurity. Students engage with cutting-edge technologies, tools, and methodologies, ensuring they graduate with relevant and marketable skills that meet the demands of the rapidly evolving cybersecurity landscape.

2.5. Student outcomes

The program's learning outcomes are designed to equip students with a diverse skill set essential for success in the field of computer science, with a focus on cybersecurity and forensics. Students will learn the following:

Students Outcomes (SOs)	
SO1:	Analyze complex computing problems and apply principles of computing and other relevant disciplines to identify solutions.
SO2:	Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
SO3:	Communicate effectively in a variety of professional contexts.
SO4:	Recognize professional responsibilities and make informed judgments autonomously in computing practice based on legal and ethical principles.
SO5:	Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline and beneficial to the community.
SO6:	Apply security principles and practices to maintain operations in the presence of risks and threats.
SO7:	Apply qualitative or quantitative study, investigative, and research methods and techniques independently and collaboratively across a wide spectrum of current and emerging cybersecurity topics.
SO8:	Explain cybersecurity and forensics foundations, principles, concepts, procedures, methodologies, operations, policies, techniques and technologies.

Overall, the Bachelor's Degree in Cybersecurity provides students with a comprehensive education that combines theoretical foundations, practical skills, and specialized knowledge, empowering them to become effective cybersecurity professionals capable of addressing the ever-changing threats facing digital systems and networks.

3. Admission Requirements

UPM serves as a gateway for students aiming to embark on their academic journey at the university. To ensure a smooth transition and readiness for undergraduate studies in Cyber Security and Forensic Computing, prospective students must meet specific admission criteria which are as follows:

3.1. High School Certificate or Equivalent

Prospective students must hold a high school certificate or its equivalent, either from the Kingdom of Saudi Arabia or from an accredited institution abroad.

3.2. Recent High School Certificate

High school certificates should not exceed five years from the date of issuance. Exceptions to this requirement may be considered by the University Council based on individual cases.

3.3. Qiyas Test Grades

Applicants may be required to demonstrate appropriate scores in both aptitude and achievement tests, if applicable, as part of the admission process.

3.4. Good Conduct

Applicants are expected to exhibit good conduct, reflecting the values and principles upheld by the university community.

3.5. Academic and Disciplinary Record

Prospective students must not have been previously dismissed from any educational institution for academic or disciplinary reasons. Any discovery of prior dismissal may result in the cancellation of admission.

3.6. Medical Fitness

Applicants should undergo a medical examination to ensure they meet the university's health requirements.

3.7. Placement Test

Applicants should undergo an English placement test to determine the level of English courses which will be the start of their Preparatory Year.

3.8. Enrollment in Preparatory Year

Enrollment in the Preparatory Year is a prerequisite for students who require additional support in English, math and computing skills before fully enrolling in their chosen program. During this preparatory period, students focus on strengthening their language proficiency in quarter based English courses alongside mathematics basic skills and computer literacy. To ensure students acquired the necessary skills and knowledge to succeed in their academic endeavors, they have to satisfy the requirements of the following courses:

Code	Course Name	Credits
ENGL 001	Preparatory English I	4
ENGL 002	Preparatory English II	4
ENGL 003	Preparatory English III	4
ENGL 004	Preparatory English IV	4
ENGL 005	Preparatory English V	4
MATH 001	Preparatory Math for Science I	4
MATH 002	Preparatory Math for Science II	4
PCS 001	Preparatory Computer Skills	3

Upon successful completion of the Preparatory Year, students are equipped with the foundational competencies needed to confidently transition into their desired program of study.

These admission requirements serve as a foundation for selecting candidates who demonstrate the academic preparedness, ethical conduct, and potential for success within the Program at UPM.

4. Graduation Requirements

To earn a Bachelor's degree in Cyber Security and Forensic Computing, students must complete a comprehensive curriculum that equips them with the necessary knowledge and skills to succeed in this dynamic field. The program is designed to provide students with a solid foundation in cybersecurity principles, technologies, and practices, while also allowing for specialization in specific areas of interest. Below are the specific requirements students must fulfill to earn their Bachelor's degree in cybersecurity:

4.1. Foundational Courses

Our foundational curriculum spans across a diverse range of disciplines essential to our program, including computer science, mathematics, English, Arabic, probability and statistics, software engineering, and artificial intelligence. This unique integration of subjects ensures a well-rounded education that equips students with the necessary skills and knowledge for success in the field. In total, there are 19 core courses, amounting to 68 credits.

Code	Course Name	Credits
MATH 101	Calculus I	4
ENGL 101	First Year Composition	3
CS 111	Introduction to Computing and Programming	4
MATH 102	Calculus II	4
ENGL 102	Introduction to Report Writing	3
CS 232	Computer Networks	4
CS 112	Object Oriented Programming	4
ENGL 201	Technical Writing	3
CS 201	Introduction to Discrete Systems	3
CS 221	Fundamentals of Operating Systems	4
CS 211	Data Structures and Algorithms	4
STAT 232	Probability and Statistics	3
SE 262	Software Engineering	3

CS 224	Computer Architecture and Organization	3
CS 317	Web Application Development	3
CS 351	Fundamentals of Database Systems	4
AI 381	Artificial Intelligence I	3
GIAS 101	Islamic Culture	3
GIAS 102	Arabic Language Skills	3

4.2. Core Courses

These core courses are essential for students aiming for a bachelor's degree in cybersecurity and forensics degree. Over the span of four years, students must fulfill the requirements of completing 16 foundational courses, amounting to a total of 46 credits. Additionally, these courses encompass a capstone project or internship, allowing students to gain practical experience and apply their knowledge in real-world situations.

Code	Course Name	Credits
FC 112	Introduction to Cyber Security	3
FC 281	Offensive Security and Ethical Hacking	4
FC 254	Operating System Hardening	3
FC 331	Software Security	3
FC 315	Ethics and Professionalism in Cyber Security	2
FC 302	Introduction to Digital Forensics	4
FC 312	Web Application Security	4
FC 362	Cyber Security Risk Management	3
FC 322	Advanced Cryptography	3
FC 394	Summer Practical Training	1
FC 491	Capstone Project I	3
FC 403	Advanced Digital Forensics	4

FC 407	Security and Privacy Standards and Policies	3
FC 492	Capstone Project II	3
FC 383	Advanced Secure Network Design	3
FC 382	Defense Mechanisms	3

4.3. Elective Courses

Students have the freedom to select elective courses according to their interests or career objectives. These electives offer a variety of specialized topics and encompass diverse disciplines, including computer science, humanities, arts, languages, social science, and foundational courses in cybersecurity. Students can choose up to 18 credits, which typically equate to 6 courses, allowing them to customize their education and pursue their individual passions within and beyond the field of cybersecurity.

Code	Course Name	Credits
GHAL xxx	Humanities, Arts, and Languages	3
FC xxx	Professional Elective I	3
FC xxx	Professional Elective II	3
GSOS xxx	Social Sciences	3
C3S xxx	College Elective I	3
C3S xxx	College Elective II	3
SE 495	Introduction to Cloud computing and Security	3

4.4. Minimum GPA

Students need to maintain a minimum GPA (Grade Point Average) of 2.0 throughout the program to remain in good academic standing and to graduate.

4.5. Total Credits

Students are required to complete a total of **132** credits to graduate. These credits encompass all the courses taken throughout a 4 year program. These credits will come from a combination of core courses, electives, general education requirements, and capstone project

4.6. Grading System

The grading system at UPM provides standardized measurements to assess students' levels of understanding in various subjects. Grading can be represented using letters (A, B, C, D, E, F), numerical values (1-4), or descriptive terms (e.g., Excellent, Very Good, Good, Pass, Weak). The following table outlines the grading system as per the University's Examination Rules and Regulations Lists:

English Descriptive	Points	Grade Limit Code	Code
Exceptional	4.00	100 – 95	A+
Excellent	3.75	90 less than 95	A
Superior	3.50	85 less than 90	B+
Very Good	3.00	80 less than 85	B
Above Average	2.50	75 less than 80	C+
Good	2.00	70 less than 75	C
Pass-High	1.50	65 less than 70	D+
Pass	1.00	60 less than 65	D
Fail	-	Less than 60	F
In-Progress	-	-----	IP
Incomplete	-	-----	IC

Denial	-	-----	DN
No Grade-Pass	-	60 and more	NP
No Grade-Fail	-	Less than 60	NF
Withdrawn	-	-----	W
Withdrawn with Pass	-	-----	WP
Withdrawn with Fail	-	-----	WF
Audit	-	-----	AU

5. Course Descriptions

Students have two distinct academic pathways to consider: the first option allows students to broaden their educational experience by choosing diverse courses within levels alongside 2 months **Summer Practical Training (FC394)**, while the second option allows students to pursue a pathway that emphasizes immersive, practical training through 6 months **Coop Practical Training (FC 493)**. This hands-on approach is tailored to deepen practical skills and enhance expertise in these crucial areas; hence the structure of the plan shifts to accommodate FC 493 (A recommended Coop plan appended in [section 10.1](#)). Below is a detailed standard study plan for students opting for the first pathway.

5.1. First Level (Total Credits:17)

MATH 101 - Calculus I	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: MATH 002	Co-requisites: N/A
Description: This course is designed to cover the basic concepts and methods of Calculus. It includes limits, continuity, and differentiability of functions of a single variable: polynomial, exponential, trigonometric, hyperbolic, and their inverses. Applications: related rates, local linear approximation, differentials, curve sketching and optimization problems. During the course, students will learn to recognize and express mathematical ideas graphically, numerically and in writing.	
ENGL 101 - First Year Composition	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: ENGL 005	Co-requisites: N/A
Description: Students are exposed to different genres of reading material, such as encyclopedias, magazines, newspapers, and websites. They are taught strategies for dealing with each genre independently and effectively. The writing component teaches argumentation and such rhetorical modes as definition writing, description, exemplification, causal analysis, and comparison. Students are taught the writing process and introduced to paragraphing, cohesion, conciseness, unity, and the use of specific details. They are alerted to common errors in grammar and sentence structure. The vocabulary component is based on the Academic World List, a corpus of vocabulary items	

based on the most frequently occurring lexis in a broad range of academic texts. In addition, students are expected to deliver short presentations on a variety of topics.

GIAS 101 - Islamic Culture

Core/Elective: Core

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

The course deals with the concept of culture linguistically and idiomatically, its relationship to civilization, and the relationship of Islamic culture with other cultures, and the course also includes the concept of the Islamic faith, its characteristics, and its effects on the individual and society, reviewing faith, its pillars, and the fruits of faith in each corner. The course also includes the concept of worship, its pillars, and conditions, in addition to that the course highlights On ethics and its place in Islam, and models of its applications in life.

GHAL xxx - Humanities, Arts, and Languages

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

The Humanities, Arts, and Languages (GHAL xxx) course offers an interdisciplinary exploration of human culture, artistic expression, and languages. Students will study historical, philosophical, and literary contexts; engage with various art forms; and enhance their language skills, deepening their understanding of cultural nuances. Through lectures, discussions, and hands-on projects, the course aims to develop critical thinking, aesthetic appreciation, and global awareness.

CS 111 - Introduction to Computing and Programming

Core/Elective: Core

Credit Hours: 4

Pre-requisites: PCS 001

Co-requisites: N/A

Description:

This course has two main objectives. Firstly, it introduces learners to the field of computer science, covering computing logic, basics of data representation, computer organization, problem-solving techniques, and algorithm writing. Secondly, it introduces programming concepts using Python, a high-level programming language. Students will learn how to design,

code, and debug computer programs, covering basic constructs such as conditions, iterations, and functions. No prior programming knowledge is necessary.

5.2. Second Level (Total Credits 18)

MATH 102 - Calculus II	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: MATH 101	Co-requisites: N/A
Description: This course is a continuation of Math 101. Topics covered include definite and indefinite integrals of functions of a single variable. Fundamental Theorem of Calculus. Techniques of integration. Applications of the definite integral to area, volume, arc length and surface of revolution. Improper integrals. Sequences and series: convergence tests, integral, comparison, ratio, and root tests. Alternating series. Absolute and conditional convergence. Power series. Taylor and Maclaurin series, Parametric function.	
ENGL 102 - Introduction to Report Writing	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: ENGL 101	Co-requisites: N/A
Description: This course teaches students how to write a term report on a themed topic. Students select individual topics within themes assigned and approved by the teacher. They are introduced to basic research skills involving the internet and the University's available databases or print collections. They are taught about research report design: the MLA (Modern Language Association) style of documentation and citation, evaluating sources, summarizing, outlining, note taking, drafting, revising and editing. Academic integrity in report writing is strongly emphasized. Students' reading skills are further enhanced through exposure to a variety of reading materials on their research topics. The ENGL 102 course also explores three common academic writing skills: paraphrasing, summary, and synthesis in report writing. Students practice writing, evaluating, and revising during the research report process. Students will advance their skills in introducing, developing, and concluding their term reports, and present them orally. Students are taught presentation skills culminating in a PowerPoint presentation based on their term report.	

CS 112 - Object Oriented Programming

Core/Elective: Core

Credit Hours: 4

Pre-requisites: CS 111

Co-requisites: N/A

Description:

The course includes principles of object-oriented programming including classes, relationships between classes, inheritance, polymorphism, encapsulation, and information hiding; Principles of object-oriented design; program debugging; error handling and documentation techniques; implementation and simple analysis of fundamental algorithms for sorting and searching; event-driven programming and the use of libraries for user interfaces.

CS 232 - Computer Networks

Core/Elective: Core

Credit Hours: 4

Pre-requisites: CS 111

Co-requisites: N/A

Description:

This course introduces the student to the study of fundamental principles in the design and implementation of computer communication networks, their protocols, and applications. Topics to be covered include layered network architectures, network applications, network programming interfaces (e.g., sockets), transport services, data link protocols, local area networks and network routing. Examples will be drawn primarily from the Internet TCP/IP protocol suite. Through homework assignments and class projects, the students will learn how the Internet works and how to design Internet applications.

FC 112 - Introduction to Cyber Security

Core/Elective: Core

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: CS 232

Description:

This course introduces students to Cyber Security, its impact and importance. Students learn about various software, hardware and network related threats, vulnerabilities and attacks. They also become familiar with different cyber threats and attacks that exploit system vulnerabilities and compromise privacy and security (i.e. confidentiality, integrity and availability). The course also covers topics (attacks and remedy) relating to Authenticity (e.g. Diffie–Hellman key exchange Keyed Hash, Digital Signature etc.), Privacy & Anonymity (e.g. Phishing, Cat

Phishing, Encryption, VPN, TOR, etc.) and Information Trustworthiness (Provenance of Information, Digital Certificate, etc.).

5.3. Third Level (Total Credits 18)

ENGL 201 - Technical Writing	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: ENGL 102	Co-requisites: N/A
Description: This course teaches students to craft a 1500-word report on a problem-solution topic related to their majors, emphasizing APA style and advanced internet research. Instruction covers audience analysis, refining topics, citations, document design, paraphrasing, summarizing, and abstract writing, alongside advanced presentation skills. The latter part of the course focuses on job application processes, including cover letters, résumés, interviews, and key business correspondence aspects like letter formats and tones, particularly for inquiry and complaint letters. It also highlights the significance of academic honesty in all forms of communication.	
CS 201 - Introduction to Discrete Systems	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: MATH 102	Co-requisites: N/A
Description: The course is intended to mainly cover the topics of fundamental mathematical structures and logical principles that are relevant to Computer Science. In this course students will be encouraged to develop an appreciation for how modern mathematics provides a sound foundation upon which to build a rich and robust understanding of the elements of computing. It also provides students with an introduction to essential elements of mathematics for computing, which include formal logic, sets, relations and functions, elementary theorem-proving methods, with an emphasis on induction, combinatorial, and graph theory.	
CS 211 - Data Structures and Algorithms	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: CS 112	Co-requisites: N/A
Description: This course discusses fundamental concepts of data structures and the algorithms that proceed from them. Topics to be covered include the implementation and use of linked lists, stacks,	

queues, trees, priority queues, heaps and graphs, with an emphasis on recursion, abstract data types, object-oriented design, and associated algorithms and complexity issues.

CS 221 - Fundamentals of Operating Systems

Core/Elective: Core

Credit Hours: 4

Pre-requisites: CS 112

Co-requisites: CS 211

Description:

This course provides an introduction to operating system design and implementation. The course will start with a brief historical perspective of the evolution of operating systems, and will further discuss the tradeoffs that can be made between performance and functionality during the design and implementation of an operating system. Particular emphasis will be given to three major OS subsystems: process management (processes, threads, CPU scheduling, synchronization, and deadlock), memory management (segmentation, paging, swapping), file systems, and operating systems protection and security.

FC 281 - Offensive Security and Ethical Hacking

Core/Elective: Core

Credit Hours: 4

Pre-requisites: CS 232, FC 112

Co-requisites: CS 221

Description:

This course provides students with an ethical perspective on the fundamentals of hacking. It covers offensive techniques used to break into or compromise systems. Understanding attacker mindsets, tools, and frameworks is essential for designing effective defenses. Students learn a wide range of attack techniques across the software stack, from reconnaissance to privilege escalation. By exploring the hacking lifecycle, they gain insights into securing systems from potential threats.

5.4. Fourth Level (Total Credits: 15)

CS 224 - Computer Architecture and Organization	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: CS 111	Co-requisites: N/A
Description: The course introduces students to the basics of modern computer organization and architecture. The topics covered include program performance, instruction sets, programming using assembly language, digital design, processor datapath and control, pipelining, memory hierarchy and parallel processors.	
SE 262 – Software Engineering	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: CS 112	Co-requisites: N/A
Description: This course introduces students to software engineering principles. The students will be exposed to software life cycle and processes. This covers requirements engineering, system analysis and design, modeling using the Unified Modeling Language (UML), and software project management. Students will have the chance to practice systems analysis and design for simple systems that serve real-world scenarios.	
STAT 232 - Probability and Statistics	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: MATH 102	Co-requisites: N/A
Description: This course covers Basic and advanced levels of Probability and statistics. The course focuses on the use of quantitative data analysis techniques for cyber security and forensic computer applications. In addition, it highlights both the Descriptive and Inferential statistical tools.	

FC 254 - Operating System Hardening

Core/Elective: Core

Credit Hours: 3

Pre-requisites: CS 221, FC 112

Co-requisites: N/A

Description:

This course covers both fundamentals and advanced topics in operating system (OS) security. It will study OS level mechanisms and policies in investigating and defending against real-world threats and attacks on computer systems, such as intrusion, boot sector virus, backdoor and stealthy rootkits. Basic OS security techniques such as authentication, system call monitoring, as well as memory protection will be discussed. Recent advanced techniques such as system-level randomization, hardware/software virtualization, and other hardware features will also be introduced.

FC 382 - Defense Mechanisms

Core/Elective: Core

Credit Hours: 3

Pre-requisites: FC 281

Co-requisites: N/A

Description:

This course introduces students to different types of Defense Mechanisms/Countermeasures, which enable administrators to secure their systems. Computers connected to networks are vulnerable to a wide range of attacks such as viruses, worms, phishing, spyware, trojan horse, buffer overflow attacks etc. Students study these attacks and are exposed to an array of defenses to protect against them. Even though the course focuses on host-based defenses, the tools and techniques that are studied are tied into other forms of network defenses (such as IPsec and Public Key Infrastructure). As such, the course takes a comprehensive view of the types of attacks that are launched against networks and computer systems, examining practical techniques and state-of-the-art tools to counter and mitigate aforementioned attacks.

5.5. Fifth Level (Total Credits: 18)

CS 317 - Web Application Development	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: CS 112	Co-requisites: CS 351
Description: This course introduces the students to the fundamentals of web applications. The course focuses on how to perform architectural planning, technology selection and how to create enterprise-level web sites that use component object model components on both the client and the server. The course also provides the student with knowledge on how to deal with the latest web technology and basic internet security.	
CS 351 - Fundamentals of Database Systems	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: CS 112	Co-requisites: N/A
Description: This course introduces the students to the concepts and design of the database. The course concentrates around core skills of organizational information requirements by modeling data using conceptual data modeling techniques, converting the conceptual data models into relational data models (database schema), and implementing in Structured Query Language (SQL). A team project that builds a database application for a real-world scenario is an important element of the course.	
FC 331 - Software Security	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: FC 112	Co-requisites: N/A
Description: The course focuses on analyzing security risks, understanding and identifying likely points of attack, and deciding how software should deal with the potential attacks. This course will teach and create awareness about possible threats in any software environment, the vulnerabilities of various applications and how to construct software that can deal with both known and unknown attacks. Some of the important topics included in this course are Identifying Security Requirements, Secure Coding, Language-based Security, Memory Exploitation, etc.	

AI 381 - Artificial Intelligence I

Core/Elective: Core

Credit Hours: 3

Pre-requisites: CS 112

Co-requisites: N/A

Description:

Artificial Intelligence (AI) is transforming how we live, work, and play by enabling new technologies such as self-driving cars or improving existing technologies such as medical diagnostics and search engines. This course will enable you to take the first step toward solving important real-world problems and future-proofing your career. This course aims to establish basic elements of theory and applications of artificial intelligence. It gives exposure to the theory behind problem solving, graph search algorithms, planning, natural language understanding, Computer vision, Robotics, machine learning, and other topics in artificial intelligence.

FC 383 - Advanced Secure Network Design

Core/Elective: Core

Credit Hours: 3

Pre-requisites: FC 382

Co-requisites: N/A

Description:

This course covers key security procedures for computer communication networks, focusing on Virtual Private Networks (VPNs), firewalls, and Intrusion Detection Systems (IDS). Topics include different types of VPNs, their architecture, implementation, and benefits. It also addresses firewall utility, construction, configuration, and administration, along with the need for comprehensive IDS. Finally, students explore Security Incident and Event Management (SIEM) solutions integrated into Security Operations Centers (SOCs). Upon completion, students gain a thorough understanding of network defense setup.

FC 315 - Ethics and Professionalism in Cyber Security

Core/Elective: Core

Credit Hours: 2

Pre-requisites: N/A

Co-requisites: N/A

Description:

The course "Ethics and Professionalism" delves into the study of morality, encompassing a careful and systematic analysis of moral decisions and behaviors while upholding ethical practices. Throughout this course, students will explore a wide range of ethical and professional issues that they may encounter during their educational and professional journey. Real-life, complex cases will be thoroughly examined to challenge students in making ethically and

professionally sound decisions, illuminating the reality that such choices are not always straightforward.

5.6. Sixth Level (Total Credits: 17)

GIAS 102 - Arabic Language Skills	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: N/A	Co-requisites: N/A
Description: This course introduces students to the fundamentals of Arabic grammar essential for reading, writing, and constructing sentences accurately. It includes a variety of exercises and texts designed to facilitate a smooth and easy learning experience.	
FC 302 - Introduction to Digital Forensics	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: FC 112	Co-requisites: N/A
Description: This course introduces students to Computer Forensics Principles and Investigation. It teaches students the methods to properly conduct a computer forensics investigation, beginning with a discussion of ethics, while mapping to the objectives of the International Association of Computer Investigative Specialists (IACIS) certification. It provides an overview of digital investigations and data recovery with emphasis on data presentation techniques and chain-of-evidence procedures. Current computer forensics tools are taught along with controls required for digital evidence. Students will be provided with an overview of the theory, best practices, and tools associated with acquiring and analyzing digital evidence.	
FC 312 - Web Application Security	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: CS 317	Co-requisites: N/A
Description: This course is designed to introduce students to the field of web security: that is, how to build secure web applications. The course covers fundamental concepts of web application and web vulnerability exploitation. State of the art tools will be used to give students pseudo practical experience with web penetration testing tools and to give them concrete examples of the concepts of the course.	

FC 362 - Cyber Security Risk Management

Core/Elective: Core

Credit Hours: 3

Pre-requisites: FC 112

Co-requisites: N/A

Description:

The cyber threat landscape is ever evolving and cyber security risks need to be considered as a continuous effort to enable better protection, detection and mitigation of attacks. This course provides an overview of the process of creating and implementing policies and procedures for responding to security incidents and for disaster recovery. The student will gain skills in creating policies for responding to security incidents as well as the business continuity and disaster recovery aspects of the incident response plan. The students will also learn cyber risk assessment and management so as to enable them to help their organizations be better prepared and more resilient against cyber threats and attacks.

FC 322 - Advanced Cryptography

Core/Elective: Core

Credit Hours: 3

Pre-requisites: STAT 232, CS 201

Co-requisites: N/A

Description:

This course covers the fundamental principles and security functions of cryptography, including classical cryptography and its mathematical foundations. It explores common cryptographic protocols and standards, differences between block and stream data, and symmetric and public key cryptography. Students learn about hash functions' importance in information security, key generation, management, exchange, and distribution, and digital signatures. Additionally, the course highlights digital certificates, PKI, and certificateless public key cryptography. Practical experience is gained through real-life applications and hands-on projects.

5.7. Summer (Total Credits: 1)

FC 394 - Summer Practical Training	
Core/Elective: Core	Credit Hours: 1
Pre-requisites: All FC3xx Courses	Co-requisites: N/A
Description: During this 2-month summer internship, students learn about cybersecurity by doing real tasks at work. Their internship provider and the career service committee have a plan for what they'll learn. Students try out the best ways of doing things in the industry. They get to use common tools, improve their skills at gathering evidence, find solutions to problems, and write detailed reports. The program focuses on being able to learn on their own, work well in teams, and use what they learn from real businesses to come up with new ideas.	

5.8. Seventh Level (Total Credits: 16)

FC 491 - Capstone Project I	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: FC254, FC282, FC331, FC383, FC302, and FC312	Co-requisites: N/A
Description: This course is the first part of a sequence of two courses that constitute the graduation capstone project. The course provides an opportunity on a hands-on project that requires the application of Analytical, Design, Forensic Investigation, and Red/Blue/Purple team skills acquired throughout the entire undergraduate cybersecurity and forensic computing curriculum. In this course, the students will work in multidisciplinary teams on selected and approved projects. The course topics cover the planning, analysis, and design phases of the projects.	
FC 403 - Advanced Digital Forensics	
Core/Elective: Core	Credit Hours: 4
Pre-requisites: FC 302	Co-requisites: N/A
Description: This advanced digital forensics course takes an extensive and profound approach into the techniques, methodologies, and tools employed in the dynamic field of digital forensics. Tailored for advanced-level students, this course is strategically designed to empower learners with the expertise and proficiency required to undertake intricate digital investigations, confront multifaceted cyber incidents, and discern elusive digital evidence. Emphasizing diverse categories of digital evidence, the course delves into coverage of network-based evidence, memory analysis, database artifacts, and more.	
FC 407 - Security and Privacy Standards and Policies	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: FC 112	Co-requisites: N/A
Description: This course builds on earlier courses and advances students' knowledge about security policies, which consist of objectives, goals, rules and formal procedures that form the foundation and structure for developing a comprehensive security program within an organization. Policy	

compliance languages are used to enforce policy compliance and restrictions within an organization. The course topics also include organizational and governmental security policies that dictate secure usage of personal and other sensitive information.

FC xxx - Professional Elective I

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

This course serves as an introduction to specialized topics that are essential to the student's chosen field. It is designed to provide a comprehensive understanding of fundamental concepts and practices. For example, in a Cyber Security and Forensic Computing program, Professional Elective examples include FC 405 and FC 494. This elective course aims to equip students with state of the art knowledge which is not included in the core courses.

FC xxx - Professional Elective II

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

This course serves as an introduction to specialized topics that are essential to the student's chosen field. It is designed to provide a comprehensive understanding of fundamental concepts and practices. For example, in a Cyber Security and Forensic Computing program, Professional Elective examples include FC 405 and FC 494. This elective course aims to equip students with state of the art knowledge which is not included in the core courses.

5.9. Eight Level (Total Credits: 12)

FC 492 - Capstone Project II	
Core/Elective: Core	Credit Hours: 3
Pre-requisites: FC 491	Co-requisites: N/A
Description: This course is the second part of a sequence of two courses that constitute the BSc graduation capstone project. In this project, the student will continue the System/Research development of the project that started in FC491. The student will deliver oral presentations, progress reports, and a final report.	
GSOS xxx - Social Sciences	
Core/Elective: Elective	Credit Hours: 3
Pre-requisites: N/A	Co-requisites: N/A
Description: The Social Sciences (GSOS xxx) course provides a comprehensive introduction to the diverse fields within the social sciences, including psychology, sociology, economics, political science, and anthropology. This course aims to equip students with an understanding of the various theories and methods used to analyze societies, human behavior, and social interactions. Through a blend of lectures, case studies, and research projects, students will explore key concepts such as social structures, economic systems, political ideologies, and cultural practices. The course emphasizes critical thinking, data analysis, and empirical research skills, preparing students for informed civic engagement and potential careers in social science-related fields.	
C3S xxx - College Elective I	
Core/Elective: Elective	Credit Hours: 3
Pre-requisites: N/A	Co-requisites: N/A
Description: This course encompasses any advanced course, typically at the 4th level or, in exceptional cases, at the 3rd level, offered by any program within the college (AI, SE) and approved by the CSFC department.	

C3S xxx - College Elective II	
Core/Elective: Elective	Credit Hours: 3
Pre-requisites: N/A	Co-requisites: N/A
Description: This course encompasses any advanced course, typically at the 4th level or, in exceptional cases, at the 3rd level, offered by any program within the college (AI, SE) and approved by the CSFC department.	

5.10. Elective Courses

The following elective courses, recognized and approved by the CSFC department, will be offered as Professional Elective I, Professional Elective II, and Humanities, Arts, and Languages Elective (GHAL xxx).

FC 405 - Incident Response	
Core/Elective: Elective	Credit Hours: 3
Pre-requisites: FC 112	Co-requisites: N/A
Description: This course introduces students to technical and nontechnical aspects of incident response. It focuses on the standards and technologies used to establish organization structures that will support information technology incident response, business continuity and disaster recovery efforts. Topics include the development and implementation of incident response, business continuity and disaster recovery plans, attack traffic analysis, and network based and host-based hardware and software. Students will learn how to produce quality reports and communicate the technical contents to a variety of audiences. Concepts will be examined and evaluated with appropriate exercises.	
FC 493 - Coop Practical Training	
Core/Elective: Elective	Credit Hours: 9
Pre-requisites: FC 491	Co-requisites: N/A
Description: This course is like a deep dive into cybersecurity and forensics for a 4 months training journey. Students learn important skills for the workplace. They follow a plan recommended by the internship provider and approved by the career service committee. The program mixes theory with hands-on projects. Students learn about industry standards and practices, using various products and services. They work on software and hardware projects, analyze data, and come up with solutions. The training lasts 600 hours spread over 15 weeks and 75 days. Students get to do practical tasks and write reports using cybersecurity terms. They also learn teamwork and how to use their experience in real-world settings. This helps them become skilled cybersecurity professionals.	

FC 494 - Python for Ethical Hacking

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: CS 111, FC 112, FC 281

Co-requisites: N/A

Description:

The course introduces the benefits of using Python in ethical hacking and gives hands-on-practice on how to develop ethical hacking tools with Python that fit particular individual or organization needs. The course provides guidance on how to build exploits, evaluate services, and automate solutions with ease using Python code. It shows a step-by-step guidance on how to develop Python codes that can scan a network, spoof ARP packets, sniff on packets, detect ARP spoofing attacks, bypassing HTTPS requests sent by victim, develop a keylogger code, scan vulnerabilities, and hack web application. It also guides students on how to setup the environment for developing ethical hacking codes with Python including installation of: Virtual Box, Kali Linux VM, MS Edge Windows 10 VM, and Pycharm as Python IDE.

FC 409 - AI for Cybersecurity

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: FC 382

Co-requisites: N/A

Description:

The "AI for Cyber Security" course is a 15-week program merging theory with hands-on practice. It covers AI and ML's role in cybersecurity, progressing from basics to advanced topics. Theoretical lectures span AI fundamentals, Python for AI in cybersecurity, data mining, malware detection, network security, natural language processing, deep learning, generative AI, and legal/ethical considerations. Labs offer practical experience in AI and ML techniques, including malware classification, network intrusion detection, spam/phishing detection, authentication attacks, and AI-driven security solutions. The course aims to equip students with a comprehensive understanding of leveraging AI and ML to enhance cybersecurity measures, detect and mitigate threats, and navigate evolving digital security challenges.

SE 495 - Introduction to Cloud computing and Security

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

This course is provided by the Software Engineering department and recognized by the CSFC department as an approved elective course. This course covers Cloud Computing fundamentals and security, starting with its definition, advantages, and cloud solutions like resource provisioning and usage-based pricing. It explores cloud service and deployment models (public, private, hybrid, community; IaaS, PaaS, SaaS), along with Cloud Economics, Billing, and Pricing. The course covers cloud architecture topics, including network provisioning, cloud databases, and queuing services. It also explores cloud security challenges and strategies, along with technical considerations for cloud migration, testing, and management. Students will engage in hands-on labs and projects using AWS, focusing on tools such as AWS IAM, Amazon VPC, and AWS EC2 to apply their learning.

FC 498 - Auditing Information Security Management System

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: FC407

Description:

In this comprehensive course on Auditing Information Security Management Systems (ISMS), students will gain a deep understanding of the crucial role that information assurance plays in safeguarding organizational assets. Through a meticulous examination of the CIA triad (Confidentiality, Integrity, and Availability), students will learn how to evaluate and ensure compliance with industry best practices, international standards, and legal requirements pertaining to information security. The course will cover different types of audits, including internal audits, external audits, and certification audits, enabling participants to understand the nuances and objectives of each. Additionally, students will acquire insights into the competence and qualifications required for auditors to effectively assess and evaluate ISMS. The course will provide a practical framework for auditing ISMS, focusing on key areas such as risk management, incident response, access controls, and vulnerability assessments. By the end of the course, participants will possess the necessary skills to perform comprehensive audits, assess the effectiveness of security controls, and contribute to the continuous improvement of information security practices within their organizations.

499 - Hardware Hacking

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: FC 281

Co-requisites: N/A

Description:

This course provides an in-depth introduction to the field of hardware security, emphasizing hands-on skills in hardware hacking. Beginning with an overview of Industrial Control Systems (ICS) and the proliferation of sensors and actuators, the course delves into reverse engineering principles, data collection, and analysis techniques to identify hardware vulnerabilities. Students will learn about specification development, various hardware modification techniques, and methods for detecting alterations. The course also covers common hardware standards, stimulation methods, functional decomposition, and the definition and enumeration of interfaces. Furthermore, the course equips students with the knowledge to protect hardware systems against threats and fosters a practical understanding of hardware from a hacker's perspective.

GHAL 103 – FOREIGN LANGUAGE (FRENCH LANGUAGE I)

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

This course for beginners allows students to acquire the basics to begin communicating and expressing themselves in French. It aims to develop, in a structured and progressive way, the four language skills of listening, speaking, reading and writing to satisfy social and professional exchanges in various contexts. Students also build knowledge of French grammar and vocabulary, which directly enhances their ability to perform tasks in the four language skills.

GHAL 203 – FOREIGN LANGUAGE (FRENCH LANGUAGE II)

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

GHAL 203 builds on the language skills students have learned in GHAL 103. GHAL 203 enables learners to develop a higher level of listening and reading comprehension, apply more specialized vocabulary and grammatical functions, and write more extensively on situations in

the hotel, catering and tourism fields. Students also demonstrate greater competence in verbal and non-verbal communication skills while becoming familiar with French culture.

GHAL 213 – FOREIGN LANGUAGE (FRENCH LANGUAGE III)

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

GHAL 213 is the continuation of GHAL 203, in which students interact orally and in writing in realistic situations to develop their communicative competence in French. The course also reinforces learners' grammar and vocabulary through video sequences on the lives of French professionals, to prepare students for the specialized skills required in the sectors of hospitality and tourism.

GSOS 214 – Work and Society

Core/Elective: Elective

Credit Hours: 3

Pre-requisites: N/A

Co-requisites: N/A

Description:

This course is designed to familiarize students with professional ethics and their significance in enhancing workplace productivity and contributing to the economic development of society. It covers key professional misconducts and strategies to address them, along with ethical practices applicable to various occupational systems. Additionally, the course explores the principles of professional ethics within the Islamic context, aiming to foster the growth of dynamic human societies.

6. Advising and Support Services

Within our academic community, we prioritize the success of our students. We recognize that navigating through your studies can sometimes be challenging, which is why we offer a range of support services to assist students in their journey.

6.1. Academic Advising

Our team of academic advisors is dedicated to providing support and guidance to students throughout their academic endeavors. Whether students are exploring their course options, planning their schedules, or seeking advice on academic matters, our advisors are here to help. They can offer personalized assistance to ensure that students make informed decisions about their academic path and stay on track towards achieving their goals.

6.2. Faculty Office Hours

Our faculty members are committed to supporting students both inside and outside the classroom. They hold regular office hours to provide additional assistance and guidance. During these office hours, students have the opportunity to engage with their professors, ask questions, and seek clarification on course material. Building relationships with professors can enhance the learning experience and offer valuable mentorship opportunities.

6.3. Resources for Success

We offer a variety of resources to help students succeed in their program:

- **Tutoring Services:** Students who find themselves struggling with coursework can benefit from our tutoring services. Our tutors are knowledgeable in a wide range of subjects and can provide support to help students understand difficult concepts, improve their study skills, and boost their confidence.
- **Career Counseling:** Planning for the future is an important aspect of the educational journey. Our career counseling services are designed to help students explore their interests, strengths, and goals. Whether students are considering potential career paths, preparing for interviews, or seeking advice on resumes and cover letters, our counselors are here to provide guidance and support.
- **Internship Opportunities:** We understand the value of gaining practical experience in the field of study. That's why we offer internship opportunities to help students apply their classroom learning in real-world settings. Internships provide hands-on experience, networking opportunities, and valuable insights into potential career paths.

6.4. English Language Support Center

The purpose of the English Language Support Center at UPM is to address the varying English proficiency levels among students interested in enrolling in our bachelors degree program of cyber security and forensic computing. Successful completion of either the IELTS or TOEFL exams enables direct enrollment into the program. Moreover, students can be exempted from English language studies in the Preparatory Year if they achieve passing scores in internationally recognized English language tests, such as a minimum score of 5 in the IELTS, 500 in the TOEFL, or meet the requirements of the Michigan testing system. Additionally, students may qualify for exemption if they attain the necessary score in any other accredited standardized international test acknowledged by the university.

Some students may come from backgrounds where their English skills require improvement. In recognition of this need, the English Language Center offers tailored assistance to help students master their English language abilities. Through specialized programs and resources, the center aims to provide students with the necessary linguistic foundation to thrive academically and professionally within the cybersecurity field. By bridging the gap in English proficiency, the center ensures that all students, regardless of their initial skill level, have the opportunity to excel in their studies and fully participate in our program at UPM.

6.5. Arabic Language Support Center

The purpose of the Arabic Language Support Center at UPM is to cater to the diverse linguistic needs of our student body, which includes a significant number of non-Arabic speakers. By providing specialized support in learning Arabic, the center aims to facilitate the integration and cultural immersion of these students within the university community. Through tailored language programs and resources, the center strives to empower students with the necessary linguistic skills to navigate academic, social, and professional contexts where Arabic proficiency is advantageous. Ultimately, the center serves as a bridge to connect students from diverse backgrounds, fostering a more inclusive and enriching educational experience at UPM.

6.6. Counseling Center

The Counseling Center at UPM is dedicated to providing comprehensive psychological, social, and behavioral support to all students, with a particular focus on those with special needs. Through direct psychological and social sessions, the center aims to address a wide range of student concerns and promote holistic well-being. Following are the key objectives of this center:

1. **Understanding Student Needs:** The center emphasizes understanding each student's personality, abilities, inclinations, and developmental stage. By gaining insight into

individual requirements, the center can tailor its support to effectively meet the diverse needs of students.

2. **Overcoming Challenges:** Through individual and group sessions, the center assists students in overcoming various challenges, including psychological, social, behavioral, and family-related issues. These sessions aim to empower students to confront their problems, alleviate fear and anxiety, and develop effective coping strategies.
3. **Building Self-Confidence:** One of the primary goals of the Counseling Center is to help students build self-confidence and trust in their abilities and skills. By providing guidance and support, the center encourages students to recognize their strengths and capabilities, fostering a positive self-image.
4. **Promoting Social Connections:** The center actively promotes the development of positive relationships with peers, teachers, and other members of the university community. Through social and educational initiatives, students are encouraged to engage in meaningful interactions within a supportive environment.
5. **Parental Engagement:** The Counseling Center facilitates communication with parents to address students' difficulties stemming from financial constraints or challenging family circumstances. By involving parents in the support process, the center strives to create a cohesive support network that enhances student well-being.

Overall, the Counseling Center plays a pivotal role in nurturing the holistic development of students at UPM. By providing a range of services and programs tailored to individual needs, the center ensures that students receive the necessary support to thrive academically, socially, and emotionally throughout their university journey.

6.7. Scholarship Unit

The Scholarship Unit at UPM serves as a vital resource for students seeking information about available scholarships within the university. With a commitment to supporting students in their academic endeavors, the unit offers a range of services designed to streamline the scholarship application process and provide ongoing support to scholarship recipients.

Key Responsibilities:

1. **Scholarship Application Management:** The unit is responsible for receiving scholarship applications from students and accurately recording them in the system. This ensures that all applications are properly documented and processed in a timely manner.
2. **Application Review and Evaluation:** Scholarship applications are carefully reviewed and evaluated by the unit to assess the eligibility and suitability of applicants. Through this process, the unit determines scholarship percentages based on each student's academic and financial status.

3. **Contract Management:** Upon approval of scholarship applications, the unit facilitates the signing of scholarship contracts between the university and the recipients. Additionally, the unit oversees the proper implementation of scholarship agreements and provides ongoing support to scholarship recipients.
4. **Monitoring and Updates:** The Scholarship Unit maintains regular communication with scholarship recipients to provide updates on any changes or developments related to their scholarships. This includes monitoring students' academic progress and ensuring compliance with scholarship requirements.
5. **Information Dissemination:** Keeping students informed about available scholarships and relevant updates is a priority for the unit. Through various communication channels, including email notifications and informational sessions, the unit ensures that students have access to timely and accurate information about scholarship opportunities.

By effectively managing scholarship applications, providing ongoing support to recipients, and facilitating communication with students, the Scholarship Unit plays a crucial role in promoting access to higher education and supporting student success at UPM.

7. Policies and Procedures

UPM maintains a comprehensive set of procedures and policies overseen by various vice rectorates, departments, and student affairs, ensuring the smooth functioning of academic and administrative processes. These include:

Vice Rectorate for Executive Affairs:

- **Code of Conduct:** Upholds ethical standards and organizational values within the university community.

Vice Rectorate for Academic Affairs:

- **Field Training Manual (Internship):** Guides students through practical training experiences.
- **Handbook for Teaching and Learning:** Provides guidelines for effective teaching methodologies.
- **UPM Manual for Development of a New Academic Program and Curriculum Review:** Ensures the quality and relevance of academic programs.

Accreditation and Quality Assurance Department:

- **UPM Quality Assurance Manual V 2.1:** Ensures adherence to quality standards and continuous improvement in educational practices.

Public Relation Department:

- **Publication Policy:** Oversees the dissemination of information and communication strategies.

Human Resources Department:

- **Code of Conduct:** Establishes ethical guidelines for employees.
- **Conflict of Interest Agreement- Updated:** Manages conflicts of interest among staff members.
- **Full-time Faculty Workloads and Working Hours:** Ensures fair and equitable workload distribution.
- **Faculty and Staff Community Service:** Encourages community engagement and service initiatives.

Student Affairs Policies and Procedures:

- **Academic Advisor Guidelines:** Provides support and guidance for academic planning and career development.
- **Admission and Registration Policies Manual:** Defines procedures for student enrollment and registration.
- **Code of Conduct:** Outlines behavioral expectations and responsibilities of students.
- **Student Disciplinary Regulations:** Ensures compliance with university rules and regulations.
- **Student Handbook:** Provides essential information and resources for student success.
- **Students Rights and Duties Deanship of Student Affairs:** Advocates for student rights and responsibilities.
- **UPM Explanatory Implementation for the Rules Regulations of Undergraduate Study Examinations:** Clarifies examination policies and procedures.
- **Student Grievance and Appeals:** Facilitates resolution of student grievances and appeals.

These policies and procedures serve to maintain transparency, fairness, and accountability within the university community, fostering an environment conducive to learning, growth, and academic excellence. You can find all their details from the following web links:

- **UPM Policies and Procedures**
<https://www.upm.edu.sa/en/upm-policies-and-procedures>
- **Student Affairs Policies and Procedures**
<https://www.upm.edu.sa/en/student-affairs-policies-and-procedures>

8. Student Resources

As part of our commitment to student success and holistic development, we offer a range of resources to support students in their academic pursuits and extracurricular interests. From state-of-the-art facilities to vibrant student organizations, our campus provides a conducive environment for learning, research, and personal growth.

8.1. Library

Our library is a hub of knowledge and information, providing students with access to a vast collection of resources, including books, journals, periodicals, and electronic databases. Whether you're conducting research for a class assignment or exploring topics of personal interest, our library offers a quiet and comfortable space for study and reflection. Knowledgeable librarians are available to assist you in finding resources and navigating academic databases.

8.2. Computer Labs

Equipped with the latest technology and software, our computer labs provide students with access to essential tools for coursework, research, and project work. Whether you need to access specialized software for your major or require additional computing resources for multimedia projects, our computer labs offer a collaborative and supportive environment for academic endeavors.

8.3. Research Centers

Our research centers serve as hubs of innovation and discovery, fostering interdisciplinary collaboration and advancing knowledge in key areas of study. Our research centers offer opportunities for hands-on research experience, mentorship from faculty experts, and access to cutting-edge facilities and equipment in the field of cyber security and forensics.

8.4. Student Organizations Related to Cybersecurity

For students interested in cybersecurity, we offer a variety of student organizations and clubs dedicated to exploring this dynamic field. These organizations provide opportunities for networking, professional development, and hands-on learning experiences. Whether you're a novice looking to learn the basics or an experienced practitioner seeking to deepen your expertise, our cybersecurity-related student organizations offer a supportive community where you can connect with like-minded peers and engage in activities such as workshops, competitions, and guest lectures.

8.5. Transportation Services

At UPM, we recognize the importance of ensuring equal access and opportunities for all students across our campuses. Certain courses may require male students to visit the female campus, and vice versa, to attend various classes or events on different campuses. To facilitate seamless movement and accessibility, we provide reliable transportation services between the male and female campuses.

Our transportation services are designed to support students in their academic pursuits and extracurricular activities. By offering convenient transportation options, we aim to eliminate barriers to participation and promote inclusivity across both campuses. Whether students are attending classes, engaging in research, or participating in campus events, they can rely on our transportation services to navigate between campuses efficiently.

At UPM, we are committed to creating an environment where all students can thrive academically and personally. By providing accessible transportation services, we ensure that every student has the opportunity to fully engage in the rich academic and extracurricular experiences available at our institution. We invite students to take advantage of these resources and explore the diverse opportunities for learning, growth, and enrichment that our campuses have to offer.

9. Internship and Career Opportunities

Guidance on finding internships, co-op opportunities, and career placement services available through the university. This section may also include information about industry certifications relevant to cybersecurity professionals.

Preparing for a successful career in cybersecurity requires more than just classroom learning. That's why we offer a range of resources and support services to help students explore internship opportunities, gain hands-on experience, and transition into rewarding careers in the field.

9.1. Finding Internships and Co-op Opportunities

Our university provides guidance and support to help students find internships and co-op opportunities that align with their interests and career goals. Through workshops, networking events, and career fairs, we connect students with potential employers and industry partners seeking talented individuals to join their teams. Additionally, our career advisors offer personalized assistance, helping students polish their resumes, prepare for interviews, and navigate the internship application process.

9.2. Career Placement Services

Our career placement services are designed to support students in securing employment upon graduation. Whether you're seeking full-time positions, part-time opportunities, or entry-level roles in cybersecurity, our career advisors are here to help. From resume building to interview preparation, we provide the tools and resources you need to stand out in the job market and land your dream job.

9.3. Industry Certifications

In addition to academic coursework, industry certifications play a crucial role in advancing your career in cybersecurity. Our university offers resources and support to help students acquiring the foundational knowledge and skills needed for preparation to obtain professional certificates, such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security+. These certifications demonstrate your expertise and competency in key areas of cybersecurity, enhancing your credibility and marketability to potential employers.

At our institution, we are committed to providing students with the opportunities and support they need to succeed in their cybersecurity careers. Whether you're seeking internships, co-op opportunities, or full-time employment, our career services team is dedicated to helping you achieve your goals. By taking advantage of our resources, guidance, and industry connections, you'll be well-equipped to embark on a successful career path in cybersecurity.

10. Appendices

In this section, you'll find additional resources and supplementary information that may be helpful to students pursuing a Bachelor's degree in Cybersecurity and Forensics.

Course Code	Course Title	Credit	Prerequisite	Co Requisite	Course Code	Course Title	Credit	Prerequisite	Co requisite
		Hours					Hours		
First Year: First Semester					First Year: Second Semester				
MATH 101	Calculus I	4	MATH 002		MATH 102	Calculus II	4	MATH 101	
ENGL 101	First Year Composition	3	ENGL 005		ENGL 102	Introduction to Report Writing	3	ENGL 101	
GHAS 101	Islamic Culture	3			CS 232	Computer Networks	4	CS 111	
GHAL xxx	Humanities, Arts, and Languages Elective	3			CS 112	Object Oriented Programming	4	CS 111	
CS 111	Introduction to Computing and Programming	4	PCS 001		FC 112	Introduction to Cyber Security	3		CS 232
Total		17			Total		18		
Second Year: First Semester					Second Year: Second Semester				
ENGL 201	Technical Writing	3	ENGL 102		STAT 232	Probability and Statistics	3	MATH 102	
CS 201	Introduction to Discrete Systems	3	MATH 102		SE 262	Software Engineering	3	CS 112	
CS 221	Fundamentals of Operating Systems	4	CS 112	CS 211	CS 224	Computer Architecture and Organization	3	CS 111	
CS 211	Data Structures and Algorithms	4	CS 112		FC 254	Operating System Hardening	3	CS 221 FC 112	
FC 281	Offensive Security and Ethical Hacking	4	CS 232, FC 112	CS 221	FC 382	Defense Mechanisms	3	FC 281	
Total		18			Total		15		
Third Year: First Semester					Third Year: Second Semester				
CS 317	Web Application Development	3	CS 112	CS 351	GHAS 102	Arabic Language Skills	3		
CS 351	Fundamentals of Database Systems	4	CS 112		FC 302	Introduction to Digital Forensics	4	FC 112	
FC 331	Software Security	3	FC 112		FC 312	Web Application Security	4	CS 317	
AI 381	Artificial Intelligence I	3	CS 112		FC 362	Cyber Security Risk Management	3	FC 112	
FC 383	Advanced Secure Network Design	3	FC 382		FC 322	Advanced Cryptography	3	STAT 232, CS 201	
FC 315	Ethics and Professionalism in Cyber Security	2							
Total		18			Total		17		
FC 394	Summer Practical Training	1	All FCxxx Courses						
Fourth Year: First Semester					Fourth Year: Second Semester				
FC 491	Capstone Project I	3	FC 254, FC 282, FC 331, FC 383, FC 302, and FC 312		GSOS xxx	Social Sciences Elective	3		
FC 403	Advanced Digital Forensics	4	FC 302		FC 492	Capstone Project II	3	FC 491	
FC 407	Security and Privacy Standards and Policies	3	FC 112		C3S xxx	College Elective I	3		
FC xxx	Professional Elective I	3			C3S xxx	College Elective II	3		
FC xxx	Professional Elective II	3							
Total		16			Total		12		
Total Credits Required: 132									

Course Code	Course Title	Credit	Prerequisite	Co Requisite	Course Code	Course Title	Credit	Prerequisite	Co requisite
		Hours					Hours		
First Year: First Semester					First Year: Second Semester				
MATH 101	Calculus I	4	MATH 002		MATH 102	Calculus II	4	MATH 101	
ENGL 101	First Year Composition	3	ENGL 005		ENGL 102	Introduction to Report Writing	3	ENGL 101	
GLAS 101	Islamic Culture	3			CS 232	Computer Networks	4	CS111	
GHAL xxx	Humanities, Arts, and Languages Elective	3			CS 112	Object Oriented Programming	4	CS 111	
CS 111	Introduction to Computing and Programming	4	PCS 001		FC 112	Introduction to Cyber Security	3		CS 232
Total		17			Total		18		
Second Year: First Semester					Second Year: Second Semester				
ENGL 201	Technical Writing	3	ENGL 102		STAT 232	Probability and Statistics	3	MATH 102	
CS 201	Introduction to Discrete Systems	3	MATH 102		SE 262	Software Engineering	3	CS 112	
CS 221	Fundamentals of Operating Systems	4	CS 112	CS 211	CS244	Computer Architecture and Organization	3	CS 111	
CS 211	Data Structures and Algorithms	4	CS 112		FC 254	Operating System Hardening	3	CS 221	FC 112
FC 281	Offensive Security and Ethical Hacking	4	CS 232, FC 112		FC 382	Defense Mechanisms	3	FC 281	
					GSOS xxx	Social Sciences Elective	3		
Total		18			Total		18		
Third Year: First Semester					Third Year: Second Semester				
CS 317	Web Application Development	3	CS 112	CS 351	GLAS 102	Arabic Language Skills	3		
CS 351	Fundamentals of Database Systems	4	CS 112		FC 302	Introduction to Digital Forensics	4	FC 112	
FC 331	Software Security	3	FC 112		FC 312	Web Application Security	4	CS 317	
AI 381	Artificial Intelligence I	3	CS 112		FC 362	Cyber Security Risk Management	3	FC 112	
FC 383	Advanced Secure Network Design	3	FC 282		FC 322	Advanced Cryptography	3	STAT 232, CS 201	
FC 315	Ethics and Professionalism in Cyber Security	2							
Total		18			Total		17		
Fourth Year: First Semester					Fourth Year: Second Semester				
FC 491	Capstone Project I	3	FC 254, FC 282, FC 331, FC 383, FC 302, and FC 312		FC 493	Goop Practical Training	9	FC 491	
FC 403	Advanced Digital Forensics	4	FC 302		FC 492	Capstone Project II	3	FC 491	
FC 407	Security and Privacy Standards and Policies	3	FC 112						
FC xxx	Professional Elective I	3							
Total		13			Total		12		
FC 394	Summer Practical Training	1	All FC xxx Courses						
Total Credits Required: 132									

10.2. Faculty Contact Information

For students seeking additional assistance or guidance, we've included contact information for faculty members within the Cybersecurity and Forensics program. Whether you have questions about course content, need academic advice, or want to discuss research opportunities, our faculty members are here to support you. Feel free to reach out to them via email or schedule office hours appointments for one-on-one discussions.

Faculty Contact Information		
Dr. Ahmed Showail	Dean of the College of Computer and Cyber Sciences	dcoc@upm.edu.sa
Dr. Khaled Khankan	Head of Cyber Security & Forensic Computing Department	csfc.hod@upm.edu.sa
Dr. Mohammed Zayed	Head of Computer Science Department	m.zayed@upm.edu.sa
Dr. Ahmed Elhayek	Head of Artificial Intelligence Department	a.elhayek@upm.edu.sa
Dr. Mohammed Abdur Rahman	Associate Professor	m.arahman@upm.edu.sa
Dr. Rashid Tahir	Assistant Professor	r.tahir@upm.edu.sa
Dr. Syed Sadiq	Assistant Professor	s.syed@upm.edu.sa
Dr. Abdulhakim Sabur	Assistant Professor	a.sabur@upm.edu.sa
Abdurazzaq Almiladi	Assistant Professor	a.almiladi@upm.edu.sa
Naveed Ahmad	Instructor	n.ahmad@upm.edu.sa
Mohammed Alkhatib	Instructor	m.al-khatib@upm.edu.sa
Noumaan Shah	Teaching Assistant	n.shah@upm.edu.sa
Dr. Mona Nakkar	Assistant Professor	m.nakkar@upm.edu.sa
Dr. Fatemah Alharbi	Assistant Professor	fat.alharbi@upm.edu.sa
Alaa Alharbi	Instructor	ala.alharbi@upm.edu.sa
Nora Alghamdi	Instructor	n.alghamdi@upm.edu.sa
Bayan Alamri	Instructor	b.alamri@upm.edu.sa
Wajiha Masood	Teaching Assistant	w.khan@upm.edu.sa
Malak Sabouni	Teaching Assistant	m.saboni@upm.edu.sa
Alaa Nasseif	Teaching Assistant	a.nasseif@upm.edu.sa
Haya Baqais	Teaching Assistant	h.baqais@upm.edu.sa