

Faculty of Information Technology

Cybersecurity Department

Study Plan of the Bachelor's Degree

In: Cybersecurity

Academic Year: 2025/2026

Study Plan Credit hours (132)

Type of Program: **Blended**

Major Type:

Humanities

Scientific/Technical

Science Medical

Teaching Type	Percentage of study plan hours/number	Actual Ratio
Complete Online E-Learning	20% - 10% Maximum	20%
Blended learning (for scientific majors)	50% - 30% Maximum	49.2%
Face-to-face learning (for scientific majors)	30% Minimum	30.8%

Note: The learning types of the courses are disseminated at all academic levels in the program





Department Vision

Excellence in education, learning, and scientific research, contributing to enhancing digital security and protecting cyberspace at both the local and global levels through programs that align with labor market needs and serve the community.

Department Mission

Preparing qualified and specialized professionals in the field of cybersecurity who possess the knowledge, practical skills, and research capabilities to address cyber threats targeting the public and private sectors by developing innovative solutions to current and future security challenges.

Program Mission

Preparing competitive students in the field of cybersecurity to meet the needs of the local community through scientifically and practically qualified faculty. The program ensures the ability to keep up with advancements and progress according to local and international standards while providing high-quality academic and practical courses that align with e-learning requirements.

Educational Program Objectives

1. Acquire the necessary theoretical and practical knowledge and skills in the field of cybersecurity.
2. Develop professional competencies to confidently practice their profession and compete locally and globally.
3. Engage in continuous learning and professional development amid technological advancements.
4. Prepare students to work effectively in teams while upholding ethical and professional responsibilities and addressing societal needs.

Educational Program Outcomes

Graduates of the program will have the ability to:

1. (Knowledge): Define computing principles and other related disciplines to identify solutions.
2. (Knowledge): Recognize professional responsibilities, ethical theories, and legal and social issues.
3. (Knowledge): Explain security principles and practices to maintain operations in the presence of risks and threats.
4. (Skill): Analyze computing problems to identify solutions.
5. (Skill): Design, implement, and evaluate a computing-based solution to meet specific computing requirements in the context of the program's discipline.
6. (Skill): Communicate effectively in a variety of professional contexts.
7. (Skill): Apply cybersecurity computing practices based on legal and ethical principles.
8. (Skill): Assess the severity of security risks, threats, or cybercrimes to ensure operational continuity.
9. (Competence): Work effectively as a team member or leader in activities relevant to the program's discipline.
10. (Competence): Build security knowledge and skills to maintain operations in the presence of risks and threats.



Plan Contents

The study plan for a bachelor's degree consists of a major in Cyber Security Of (132) credit hours disseminated as follows:

Sequence	Classification	Credit Hours	Percent %
1st	University Requirements	27	20%
2nd	College Requirements	18	14%
3rd	Program Requirements	87	66%
Total		132	100%

Coding System Approved by the University

4	0	5	-	-	Semester	year	-
College Code	Major Code	Knowledge domain	Course Level	Sequence			
4 Faculty of Information Technology	05 Cybersecurity						

Knowledge Domain

Domain Code	Knowledge Domain	Credited Hours of Study Plan
1	Computer Science and Algorithms: Discrete Mathematics, Data Structures, Algorithms Design and Analysis, Operating Systems.	12
2	Programming: Networks and Information Security Programming, Web Application Programming.	6
3	Fundamentals of Cybersecurity: Introduction to Cybersecurity, Digital forensics, Data and software security, Network Management and Security, System and Infrastructure Security.	15



Domain Code	Knowledge Domain	Credited Hours of Study Plan
4	Cybersecurity: Cryptography, Digital Forensics, Data Integrity and authentication, Secure communication protocols, Penetration Testing.	15
5	Supporting Knowledge Areas: Statistics, Linear Algebra.	6
6	Elective Courses: Several courses within the sub-field of the program.	9
7	Field training: 3 hours after passing a minimum of 80 credit hours.	3
8	Graduation Project (1): 2 credit hour after passing 90 credit hours. Graduation Project (2): 2 credit hours after passing graduation project (1)	4

First: University Requirements: (27) Credit Hours

A. Compulsory Requirements: (18)Credit Hours

Teaching type			Course Number	Teaching type	Credit Hours	Prerequisite
Online E-Learning	Blended	Face-to-Face				
√			50511104	Communication and Communication Skills I (Arabic)	3	50511111
√			50511105	Communication and Communication Skills I (English)	3	50511112
√			50511205	Life Skills and Social Responsibility	3	
√			50511206	National Education	3	
√			50511305	Leadership and Innovation	3	
√			50511308	Military Sciences	3	
√			50541209	Volunteer Work and Community Development	0	
			Total		18	

B. Elective Requirements: (9)Credit Hours from the following list:

Teaching type			Course Number	Teaching type	Credit Hours	Prerequisite
Online E-Learning	Blended	Face-to-Face				
√			50521106	Communication and Communication Skills 2 (Arabic)	3	50511104
√			50521107	Communication and Communication Skills 2 (English)	3	50511105



Teaching type			Course Number	Teaching type	Credit Hours	Prerequisite	
Online E-Learning	Blended	Face-to-Face					
√			50521203	Principles of Psychology	3		
√			50521204	Human Rights	3		
√			50531101	Islamic Culture	3		
√			50531205	Quds and the Hashemite Guardianship	3		
√			50541103	Computer Skills	3	5051113	
√			50541204	Development and Environment	3		
√			50541206	Health and Society	3		
√			50541208	Introduction to Sustainable Development	3	-	
√			50541211	Introduction to Artificial Intelligence	3	-	
√			50541308	Foreign Language	3		
√			50541309	Digital Culture	3	5051113	
			Total			9	

C. Remedial course: (0) Credit Hours

Teaching type			Course Number	Course Title	Credited Hours*	Theoretical	Practical	Pre-Requirement
Online E-Learning	Blended	Face-to-Face						
√			5051111	Arabic Language Basics	3		√	
√			5051112	English Language Basics	3		√	
√			5051113	Computer Basics	3		√	
			Total		0			

**Second: College Requirements: (18) Credit Hours****A. Compulsory Requirements: (18) Credit Hours**

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		40741101	Fundamentals of information technology	3	3	0	
	√		40722101	Websites Design	3	3	0	40741101
	√		50521101	Calculus I	3	3	0	
		√	50511208	Discrete Mathematics	3	3	0	50521101
	√		40733203	Operating Systems	3	3	0	40712102
		√	40713104	Algorithms Design and Analysis	3	3	0	40712102
			Total		18	18	0	

Third: Program Requirements (87) Credit Hours**A. Compulsory Requirements: (75) Credit Hours**

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		50511209	English Language for Information Technology	1	1	0	
		√	40721101	Introduction to Programming	3	3	0	
		√	40721102	Laboratory of Introduction to Programming	1	0	2	40721101 (co)
		√	40721203	Object Oriented Programming	3	3	0	40721101
		√	40721204	Laboratory of Object-Oriented Programming	1	0	2	40721203 (co)
		√	40712102	Data Structures	3	3	0	40721203
		√	40712103	Laboratory of Data Structure	1	0	2	40712102 (co)
		√	40742202	Databases	3	3	0	40712102
		√	40742203	Laboratory of Databases	1	0	2	40742202 (co)
	√		40543101	Data and software security	3	3	0	40722205
		√	40722205	Programming of Internet Applications	3	3	0	40722101-40742202 (co)



Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
		√	40743204	Computer Networks	3	3	0	40741101
	√		40541201	Introduction to Cybersecurity	3	3	0	
		√	40542102	Fundamentals of Encryption	3	3	0	40541201
		√	40543201	System and Infrastructure Security	3	3	0	40543204
	√		40543103	Information Security Protocols	3	3	0	40542102
		√	40543204	Network Management and Security	3	3	0	40743204
	√		40544221	Artificial Intelligent Applications in Cybersecurity	3	3	0	40713104
	√		40544108	Ethical Hacking	3	2	2	40543204
	√		40544218	Penetration Testing	3	2	2	40543204
		√	40544110	Networks and Information Security Programming	3	3	0	40543101
			40544213	Digital Forensics	3	2	2	40543204
	√		40542103	Data integrity and authentication	3	3	0	40721203
	√		40543202	Secure Systems Development and Design	3	3	0	40543101
	√		40543102	Cybersecurity Ethics, Risks and Policies	3	3	0	40541201
	√		40584202	Field Training	3	0	3	Complete 80 CH
	√		40594200	Applied Graduation Project (1)	2	0	2	Complete 90 CH
	√		40594203	Applied Graduation Project (2)	2	0	2	40594200
			Total		72	57	15	

* Credit Hours



B. Elective Requirements: (9) Credit Hours

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		40544112	Wireless Network Security	3	2	2	40743204
	√		40544214	Internet of Things Security	3	3	0	40743204
	√		40544215	Cloud Computing Security	3	3	0	40543103
	√		40544216	Special Topics On Cybersecurity	3	3	0	Complete 60 CH
	√		40544109	Intrusion Detection and Prevention	3	3	0	40543204
	√		40544219	Database Management Systems Security	3	3	0	40742202
	√		40544220	Emerging Topics on Cybersecurity	3	3	0	Complete 60 CH
	√		40543205	Networks Monitoring and Certification	3	3	0	40543204
	√		40543206	Electronic Commerce Security	3	3	0	40543101
			Total		9	9	0	

C. Ancillary Courses: (6) Credit Hours

Teaching type			Course Number	Course Title	Credited Hours	Theoretical	Practical	Pre-Requisite
Online E-Learning	Blended	Face-to-Face						
	√		50531100	Principle of Statistics and Probability	3	3	0	
	√		50212104	Linear Algebra (I)	3	3	0	50521101
			Total		6	6	0	



Guidance plan

First Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
40741101	Fundamentals of Information Technology	Blended	3		
40721101	Introduction to Programming	Face-to-Face	3		
40721102	Laboratory of Introduction to Programming	Face-to-Face	1		40721101
40541201	Introduction to Cybersecurity	Blended	3		
50521101	Calculus (I)	Blended	3		
	University Compulsory Requirement	Online E-Learning	3		
Total			16		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
40722101	Websites Design	Blended	3	40741101	
40721203	Object Oriented Programming	Face-to-Face	3	40721101	
40721204	Laboratory of Object-Oriented Programming	Face-to-Face	1		40721203
50511209	English Language for Information Technology	Blended	1		
50511208	Discrete Mathematics	Face-to-Face	3	50521101	
50212104	Linear algebra (I)	Blended	3	50521101	
50531100	Principle of Statistics and Probability	Blended	3		
Total			17		

* Credit Hours



Second Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40743204	Computer Networks	Face-to-Face	3	40741101	
40712102	Data Structures	Face-to-Face	3	40721203	
40712103	Laboratory of Data Structures	Face-to-Face	1		40712102
40542103	Data integrity and authentication	Blended	3	40721203	
40542102	Fundamentals of Encryption	Face-to-Face	3	40541201	
	University Compulsory Requirement	Blended	3		
Total			16		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40543204	Network Management and Security	Face-to-Face	3	40743204	
40722205	Programming of Internet Applications	Face-to-Face	3	40722101	40742202
40742202	Databases	Face-to-Face	3	40712102	
40742203	Laboratory of Databases	Face-to-Face	1		40742202
40543103	Information Security Protocols	Blended	3	40542102	
	University Compulsory Requirement	Online E-Learning	3		
Total			16		



Third Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40543205	Networks Monitoring and Certification	Blended	3	40543204	
40543101	Data and software security	Blended	3	40722205	
40733203	Operating Systems	Blended	3	40710102	
40713104	Algorithms Design and Analysis	Face-to-Face	3	40712102	
40543102	Cybersecurity Ethics, Risks and Policies	Blended	3	40541201	
	University Compulsory Requirement	Online E-Learning	3		
Total			18		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40544213	Digital Forensics	Blended	3	40543204	
40543201	System and Infrastructure Security	Blended	3	40543204	
40544110	Networks and Information Security Programming	Face-to-Face	3	40543101	
	Program Elective Requirement	Blended	3		
	University Elective Requirement	Online E-Learning	3		
	University Compulsory Requirement	Online E-Learning	3		
Total			18		



Fourth Year

First Semester					
Course No.	Course Title	Type of Learning	Credited Hours	Prerequisite	Co-requisite
40544218	Penetration Testing	Blended	3	40543204	
40543202	Secure Systems Development and Design	Blended	3	40543101	
40594200	Applied Graduation Project (1)	Blended	2	Complete 90 CH	
	University Elective Requirement	Online E-Learning	3		
	University Compulsory Requirement	Online E-Learning	3		
	Program Elective Requirement	Blended	3		
Total			17		

Second Semester					
Course No.	Course Title	Type of Learning	Credited Hours*	Prerequisite	Co-requisite
40544108	Ethical Hacking	Blended	3	40543204	
40584202	Field Training	Blended	3	Complete 80 CH	
40594203	Applied Graduation Project (2)	Blended	2	40594200	
	University Elective Requirement	Online E-Learning	3		
	Program Elective Requirement	Blended	3		
Total			14		

Courses Tree



Courses Tree

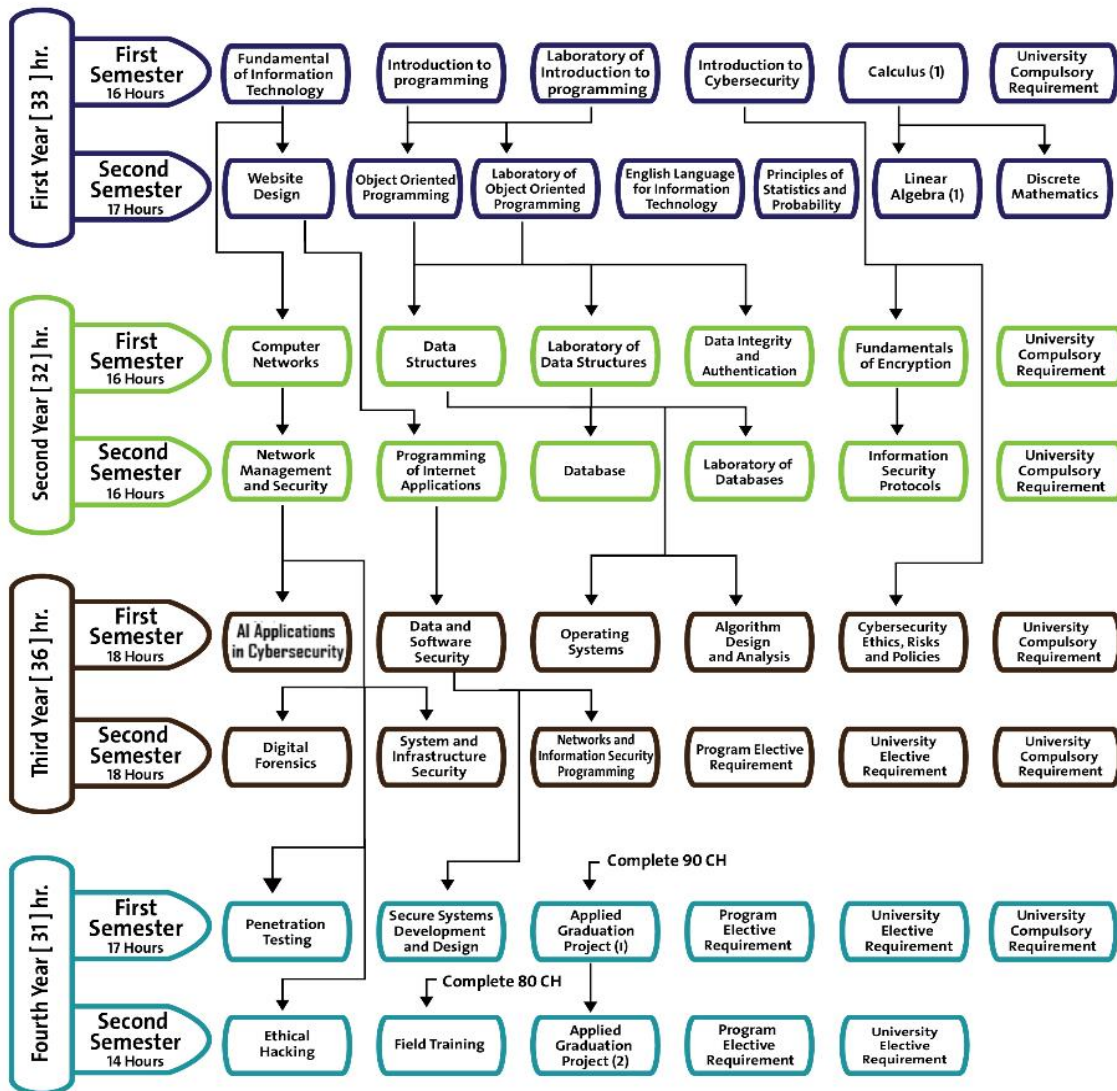
College: College of Information Technology

Department: Cyber security

Major: Cyber security Program

Program: Bachelor

Issue Number 6 - Date: 01/08/2025



F566-1, Rev. a

Ref.: Quality Assurance Council Session (08/2021-2022), Decision No.: 01, Date: 21/05/2022



F026-1, Rev. d

Ref.: Deans' Council Session (16/2025-2026), Decision No.: 11, Date 23/12/2025





Course Description

40712102, Data Structures, (3) Credit Hours, Prerequisite: 40721203 Object Oriented Programming, Face-to-Face

Basic concepts of data structure and algorithm. The topics that will be covered in this course concerning Data type and structures; Abstract data types and encapsulation; Stacks; Queues; Recursion; Linked Lists; Binary trees; General trees; File organization: sequential and indexed files; Graphs: representation, traversing, shortest path; Sorting: exchange, insertion, quick sort, heap and others; Searching. At the end of this course, students will be able to select the proper data structure and algorithm to solve a specific software problem, The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40712103, Laboratory of Data Structures, (1) Credit Hours, Co-requisite: 40712102, Face-to-Face

A practical laboratory in data structures, covering practical exercises including abstract data types and aggregation, accumulators, tuples, recursion, sequential lists, general trees, file organization, graphs, sorting and searching. The laboratory includes the completion of a practical project or research by students.

40741101, Fundamentals of Information Technology, (3) Credit Hours, Prerequisite: -, Blended

Knowledge of the terminology, information systems environment, processes, and components associated with information technology, information systems concepts, components, tools, and applications. It will provide an introductory understanding of computer hardware, numbering system and knowledge of how data is prepared for computer, instruction processed at a basic machine level, and software (operating systems, database, and web development and applications). It also introduces the networking, Internet, and the basics of the information security, web searching, in addition to algorithms and problem solving, The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40742202, Databases, (3) Credit Hours, Prerequisite:40712102 Data Structures, Face-to-Face

Basic concepts of databases and the main topics such as: database definition, database system; overview of database management, database system architecture, introduction to relational model, database algebra, database design, database integrity, an introduction to structured query language (SQL), mapping between ER- and EER-to-Relational, The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40742203, Laboratory of Database, (1) Credit Hours, Corequisite: 40742202, Face-to-Face

A practical laboratory in databases, covering practical exercises in database system and database management (relational database systems RDBMS, structured query language (SQL), and schema design techniques The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

50511208, Discrete Mathematics, (3) Credit Hours, Prerequisite: 50521101 Calculus, Face-to-Face

Fundamental aspects of discrete mathematics used in computer science starting with propositions, logical operations, truth tables, set theory, relations and functions, and methods of proofs. The course also introduces the



concepts of sequences, matrices, lattices, graph theory, and trees (rooted tree, subtree), The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40722101, Websites Design, (3) Credit Hours, Prerequisite: 40741101 Fundamentals of Information Technology, Blended

Basic concepts of the World Wide Web, internet technology, current Web protocols, and client-server programming for desktop computers and smart phones. Students will learn standard Hypertext Markup Language (HTML) for create the web pages, basics of Cascading Style Sheets (CSS) for design and layout the web pages, as well as JavaScript, together with XML and JSON for data-interchange and Ajax technology for building rich internet applications for desktop computers and smart phones. Students will apply their gained knowledge in a series of practical assignments. The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40721101, Introduction to Programming, (3) Credit Hours, Prerequisite: , Face-to-Face

The fundamental concepts of programming using selected language. It covers basic structures of programming concepts such as variables, data types, control structures, arrays, functions, and pointers. A brief introduction to classes and objects is also given. Students will apply their gained knowledge in a series of assignments. Practical work for three hours weekly is included. The course includes complete a practical project or research by the students.

40721102 Laboratory of Introduction to Programming, (1) Credit Hours, Corequisite: 40721101 Introduction to Programming, Face-to-Face

A practical laboratory in programming using selected language, where it covers practical exercises in the basics of programming such as variables, data types, control statements, matrices, functions and indicators. In this course, students apply their knowledge through a series of practical assignments in the laboratory.

50511209 English Language for Information Technology, (1) Credit Hours, Prerequisite: -, Blended

This course is designed to develop students' professional English communication skills within the context of the IT industry. It focuses on key technical vocabulary, grammar, and communication strategies used in common workplace scenarios such as giving presentations, writing emails and reports, troubleshooting IT problems, working with software/hardware, and managing online services such as websites, databases, and e-commerce systems..

40721203, Object Oriented Programming, (3) Credit Hours, Prerequisite: 40721101 Introduction to Programming, Face-to-Face

Object-oriented concepts (encapsulation, data abstraction, inheritance, and polymorphism) along with OO design using UML (unified modeling language). The OOP concepts covered using JAVA programming language. The course emphasizes on the concepts of classes, templates, friend classes, inheritance, abstract class and virtual functions, exceptions, and generic programming. Upon completion, students should be able to use an object-oriented language to develop rather complex programs The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40721204, Laboratory of Object Oriented Programming, (1) Credit Hours, Corequisite: 40721203 Object Oriented Programming, Face-to-Face





A practical laboratory in object-oriented programming, covering practical exercises in object-oriented programming (encapsulation, data abstraction, inheritance, polymorphism). The course is concerned with applying concepts of classes (classes and templates, friendly classes, inheritance, abstract layer and virtual functions, exceptions and general programming in a practical way). The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40713104, Algorithms Design and Analysis, (3) Credit Hours, Prerequisite: 40712102 Data Structures, Face-to-Face

Basic concepts of designing and analyzing algorithms. Topics covered: review of abstract data types and data structures, definition of algorithms, classifying functions and computational complexities of algorithms, algorithms analysis & design techniques including: divide and conquer greedy methods, searching and sorting, trees, graphs, hashing, combinatorial algorithms and P/NP problems, The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40543101, Data and Software Security, (3) Credit Hours, Prerequisite: 40722205 Programming of Internet Applications, Blended

This course aims to provide students with the fundamental concepts and basic methods of data security and software security within the context of modern systems and applications. It addresses the principles of protecting data in its various states (at rest, in transit, and in use) by discussing access management policies and procedures, the operation of encryption mechanisms, backup and recovery, privilege management, and data loss prevention (DLP) techniques.

The course also focuses on the foundations of software security and the integration of security into the Software Development Life Cycle (Secure SDLC), with an emphasis on secure coding practices, input validation, session management, error handling, and secure configuration of applications. In addition, it provides a general introduction to a number of common vulnerabilities in web applications and software (such as those listed in the OWASP Top 10 at an introductory level) and methods for mitigating their risks, alongside a discussion of logging, auditing, and monitoring the use of data and software in different environments.

40542103, Data Integrity and Authentication, (3) Credit Hours, Prerequisite: 40721203 Object Oriented Programming, Blended

The course provides a comprehensive overview of the integrity and authentication of data, while emphasizing the importance of cryptography in securing data and supporting its authentication processes. The course also addresses other issues, such as hardware problems, software engineering, and the social and political challenges that must be taken into account to achieve a comprehensive and effective security system. The course includes special topics such as encryption techniques. Classic and modern, data hiding methods, and the impact of human factors on authentication systems.

40722205 Programming of Internet Applications, (3) Credit Hours, Prerequisite: 40722101 Websites Design, 40742202 Databases, Face-to-Face

The knowledge and the tools to design and implement internet web applications for desktop computers and smartphones using PHP language as a server-side language. Initially, the course will introduce HTML language and web applications. Students will learn about concepts of PHP, the functionality of web servers, and install and configure Apache HTTP server or Microsoft IIS. This course goes over the syntax and usage of PHP language such



as data types, operators, arrays, control statements, expressions, sessions, cookies, as well as creating programs that interact with MySQL databases. At the end of this course, students will create and maintain a small web application project on a live web server for desktop computers and smartphones. The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40743204 Computer Networks, (3) Credit Hours, Lecture: 3, 40741101 Fundamentals of Information Technology, Face-to-Face

Key Concepts of Computer Networks; Broad Range of Topics in Networking (e.g. Networks Applications, Network Classifications and Topologies, Network Layers, Channel Performance Measures, Transmission Media, Communication Network Protocols and Architecture); Data Link Layer (e.g. Framing, Error Detection and Correction, CSMA/CD, LAN IEEE Standards); Network Layer (e.g. IP service model, IP Addressing, Sub-netting, Host Configuration DHCP, ARP Protocol, ICMP protocol); Transport Layer (e.g. UDP Protocol, TCP Protocol, TCP Reliable Transfer and Sliding Window, TCP Flow and Congestion Control); Application Layer (e.g. DNS Protocol, NAT Protocol, HTTP Protocol, Persistent and Non-Persistent HTTP Connection), The course includes an applied project through which students can practically employ the knowledge and skills they have acquired.

40733203 Operating Systems, (3) Credit Hours, Prerequisite: 40712102 Data Structures, Blended

This course covers the definition and role of the operating systems. Topics spanned functionality and structuring methods of a typical operating system; Introduction to modern operating systems, including device control, interrupts, synchronization and inter-process communication, process scheduling, memory management and virtual memory, disk management, and security. Students will apply their gained knowledge in a series of assignments.

40541201 Introduction to Cybersecurity, (3) Credit Hours, Prerequisite: -, Blended

This course aims to introduce students to the fundamental concepts of cybersecurity and information security. It covers the core principles of confidentiality, integrity, and availability; types of cyber threats and attacks; and the elements involved in protecting information assets in systems and networks.

Students are introduced to basic access control models, identity and privilege management, and an overview of cryptography and its role in data protection, in addition to security policies, procedures, and organizational controls. The course also focuses on developing security awareness and safe use practices for digital technologies, with an emphasis on the ethical and legal aspects of cybersecurity, through practical examples, applications, and case-based exercises.

40542102 Fundamentals of Encryption, (3) Credit Hours, Prerequisite: 40541201 Introduction to Cybersecurity, Face-to-Face

This course aims to introduce students to the fundamental concepts and principles of cryptography, with a focus on cryptographic algorithms and their role in ensuring the confidentiality, integrity, and authenticity of information. It covers both classical and modern cryptography, including the study of symmetric-key algorithms (such as block and stream ciphers) and asymmetric-key algorithms, as well as hash functions, message authentication codes (MACs), digital signatures, and key management and Public Key Infrastructure (PKI), supported by introductory mathematical foundations.



The course includes an applied project designed to enable students to employ cryptographic algorithms and their various components in practical scenarios related to information security.

40543201 System and Infrastructure Security, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Blended

This course aims to provide students with the fundamental knowledge and skills required for securing operating systems and the technical infrastructure of organizations, including servers, workstations, networks, and core infrastructure services such as Active Directory, name services, and email services. It covers the principles of system hardening, secure configuration management, and identity and privilege management at the system and infrastructure levels, as well as the protection of critical servers and services. The course also introduces the security of virtualized environments and cloud infrastructures.

In addition, it focuses on controls related to backup and disaster recovery, logging and monitoring, and the detection of and initial response to security incidents, thereby contributing to a comprehensive enhancement of the security posture of the organizational IT environment.

40543103 Information Security Protocols, (3) Credit Hours, Prerequisite: 40542102 Fundamentals of Encryption, Blended

This course aims to deepen students' understanding of cryptographic applications in information security protocols at the network, system, and application layers. It covers the principles and foundations underpinning the design of security protocols, such as authentication, key exchange, session management, confidentiality, integrity, and non-repudiation.

The course involves the study and analysis of a number of common security protocols, including channel security protocols (TLS/SSL), IP security (IPsec), secure access protocols (SSH, VPN), authentication protocols (Kerberos), secure email protocols (PGP/S/MIME), as well as an introductory treatment of wireless security protocols (such as WPA2/WPA3). It also discusses threat models and attacks against protocols (such as replay attacks, man-in-the-middle attacks, and impersonation), with a focus on analyzing case studies that demonstrate the consequences of insecure protocol design or implementation in real-world environments.

40543204 Network Management and Security, (3) Credit Hours, Prerequisite: 40743204 Computer Network, Face-to-Face

This course aims to provide students with the fundamental concepts and basic methods of network management and security in enterprise environments. It covers the principles of network administration and operation, performance monitoring, capacity planning, and the management of network addresses and services, in addition to an introductory overview of network management frameworks such as the FCAPS model.

The course also focuses on network security controls and tools, including firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Networks (VPNs), network segmentation and demilitarized zones (DMZs, VLANs), and defense-in-depth strategies. Furthermore, it discusses logging and monitoring mechanisms and initial response to network incidents through examples and case studies drawn from real-world work environments.

**40543205 Networks Monitoring and Certification, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Blended.**

This course aims to provide students with the knowledge and practical skills required for network monitoring and documentation in enterprise environments. It covers the concepts and objectives of network monitoring and key performance indicators (KPIs), as well as network data collection techniques such as SNMP, NetFlow/sFlow, logs, and Syslog. The course also addresses the design and implementation of a network monitoring system, the analysis of alerts and reports, and their integration with network management and security processes.

In addition, the course covers network documentation through the preparation of topology diagrams, device and service inventories, configuration and change logs, and incident and availability reports, with hands-on applications using monitoring and/or simulation tools and platforms available in the laboratory.

40544108 Ethical Hacking, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face

This course aims to introduce students to the fundamental concepts and principles of ethical hacking as an organized and authorized practice designed to improve the security of systems, networks, and applications. It focuses on understanding the attacker's mindset, common attack patterns and vulnerabilities from a defensive perspective, as well as the legal and ethical framework, the responsibilities of cybersecurity professionals, and acceptable use policies. The course includes an applied project or research-based assignment that enables students to employ the studied concepts and tools within authorized and controlled laboratory environments.

40544218 Penetration Testing, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face

This course aims to provide students with structured knowledge and practical skills in penetration testing by applying its phases according to recognized methodologies, including planning and scoping, information gathering, vulnerability discovery and exploitation in safe environments, and documenting results through technical reports and improvement recommendations. The course emphasizes adherence to legal and ethical frameworks, confidentiality requirements, and data integrity. It includes an applied project or research-based assignment in which students perform penetration testing procedures on authorized virtual systems or environments.

40544110 Networks and Information Security Programming, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Face-to-Face

This course aims to equip students with the programming skills necessary to support information and network security through the development of simple scripts and software tools used for automation, log collection and analysis, security control testing, and network traffic monitoring within authorized environments. The course relies on a high-level programming language such as Python, in addition to introductory use of scripting environments such as Bash/PowerShell, to implement practical tasks including reading and analyzing system logs, programmatically handling network protocols (sockets), performing basic service scanning, and using standard cryptographic libraries, with an emphasis on secure programming principles and adherence to relevant laws and policies.

The course includes an applied project or research-based assignment that enables students to employ the developed scripts and tools in supporting information security teams within laboratory or realistic application environments.

**40544213 Digital Forensics, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face**

This course aims to introduce students to the fundamental concepts and principles of digital forensics as a field concerned with the collection, preservation, analysis, and presentation of digital evidence in accordance with legal and procedural frameworks. The course covers the types and sources of digital evidence, the principles of the chain of custody, and the stages of the digital investigation process from preparation to documentation and reporting, in addition to an overview of legal and ethical aspects and the role of incident response teams.

The course also includes an applied project or research-based assignment that enables students to employ the studied tools and techniques in simplified digital investigation scenarios.

40543202 Secure Systems Development and Design, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Blended

This course aims to enable students to design and develop secure software systems and applications by integrating security requirements into all phases of the Software Development Life Cycle (Secure SDLC). This includes analyzing and defining security requirements, threat modeling, designing secure architectures, adopting secure design and coding patterns, and performing code review and testing from a security perspective.

The course builds on the programming skills acquired in previous courses and includes an applied project or research-based assignment in which students apply the studied concepts and techniques to a real-world system or application in the field of cybersecurity.

40543102 Cybersecurity Ethics, Risks and Policies (3) Credit Hours, Prerequisite: 40541201 Introduction to Cybersecurity, Blended

This course aims to introduce cybersecurity students to the ethical, legal, and social dimensions of computing and cybersecurity by addressing professional and ethical responsibilities, individual rights, intellectual property, information systems crimes, malware, intrusions, and methods of technology misuse. The course also introduces the concepts and stages of cybersecurity risk management, including risk assessment and analysis, exposure factors, security controls, mitigation strategies, and the management of threats and vulnerabilities.

The course further focuses on the institutional policies, procedures, and controls required to enhance cybersecurity and to build a governance framework aligned with the Jordanian National Cybersecurity Framework (JNCSF), in coordination with the National Cybersecurity Center.

40584202 Field Training, (3) Credit Hours, Prerequisite: Complete 80 CH, Blended

This course aims to provide cybersecurity students with practical professional experience through field training in an institution or organization relevant to their specialization for a period of no less than eight weeks and a minimum of 200 actual training hours. The training enables students to apply the knowledge and skills acquired during their studies in a real work environment and to participate in tasks and activities related to cybersecurity under joint supervision from the training provider and the academic department.



During the training period, the student is required to comply with the regulations and guidelines approved by the department, the faculty, and the Deans' Council, including follow-up requirements, report preparation, and evaluation by supervisors. The course contributes to enhancing students' technical and professional skills, professional ethics, and readiness for the labor market.

40594200 Applied Graduation Project (1), (2) Credit Hour, Prerequisite: Complete 90 Credit Hours, Blended

This course aims to prepare students to initiate an applied graduation project in the field of cybersecurity by selecting an appropriate topic, formulating the project problem and objectives, conducting a review of relevant literature, analyzing functional and security requirements, and designing the proposed solution and implementation plan. The course focuses on developing students' skills in applied research, project planning, and adherence to academic integrity standards. It is a prerequisite for the course "Applied Graduation Project 2."

40594203 Applied Graduation Project (2), (2) Credit Hours, Prerequisite: 40594200 Applied Graduation Project (1), Blended

This course aims to complete the implementation of the applied graduation project planned in "Applied Graduation Project 1" through building, implementing, and testing the technical solution or security system, and analyzing its results in accordance with professional and academic standards. The course includes preparing a comprehensive final report, as well as presenting and defending the project before a specialized committee, thereby enhancing students' skills in problem solving, teamwork, and professional communication in the field of cybersecurity.

40544112 Wireless Network Security, (3) Credit Hours, Prerequisite: 40743204 Computer Networks, Blended

This course aims to provide students with the fundamental concepts and methods for securing wireless networks in enterprise environments. It covers the architecture and components of wireless networks, related threat models and security vulnerabilities, and the encryption and authentication mechanisms adopted in various standards such as Wi-Fi networks. The course also addresses the analysis of major wireless network attacks and their exploitation techniques, as well as methods of mitigation through appropriate security controls and configurations, and the development of effective security policies for enterprise wireless networks.

40544214 IoT Security, (3) Credit Hours, Prerequisite: 40743204 Computer Networks, Blended

This course aims to introduce students to the architecture of Internet of Things (IoT) systems, including the types of devices, components, and protocols used, with an emphasis on understanding the specific risks and security vulnerabilities associated with such systems. It also addresses the principles and methods required to design and deploy more secure solutions for IoT devices and modules, including securing communications, protecting data, managing identity and access, and building operating environments that minimize opportunities for exploitation and attacks.

The course includes an applied project or research-based assignment that enables students to employ these concepts in practical applications or empirical studies in the field of IoT security.

40543206 Electronic Commerce Security, (3) Credit Hours, Prerequisite: 40543101 Data and software security, Blended





This course aims to introduce students to the principles of e-commerce from both business and technology perspectives, with a focus on security, privacy, intellectual property rights, and legal obligations. The course addresses client-side and server-side vulnerabilities, the operation of cryptographic protocols such as SSL, and transaction security standards such as PCI DSS, in addition to the security of web servers and their applications, access control, and database protection. Students are also introduced to concepts of defensive coding, threat modeling, and mechanisms for protecting identity and information in web and e-commerce environments.

40544215 Cloud Computing Security, (3) Credit Hours, Prerequisite: 40543103 Information Security Protocols, Blended

This course aims to introduce students to the concepts and service models of cloud computing (IaaS, PaaS, SaaS) from a security perspective, with a focus on analyzing threats and risks associated with cloud environments and understanding the respective responsibilities of service providers and customers within the shared responsibility model.

The course covers controls for securing cloud infrastructure, cloud identity and access management (Cloud IAM), and the protection of data and services through encryption, backup policies, and key management. It also reviews best practices, frameworks, and standards related to cloud security.

40544216 Special Topics on Cybersecurity, (3) Credit Hours, Prerequisite: Complete 60 CH, Blended

This course aims to deepen students' knowledge of advanced and selected topics in cybersecurity. Each semester, it focuses on contemporary issues and emerging trends that respond to developments in the field and labor market needs, such as: security of industrial control systems (ICS/SCADA), Internet of Things (IoT) security, blockchain and cryptocurrency security, cloud security, security of smart applications and autonomous vehicles, artificial intelligence threats and machine learning-based attacks, as well as other specialized topics.

The course includes the discussion of real-world case studies and the analysis of recent attacks and vulnerabilities, in addition to the use of advanced tools and techniques for testing and analysis. This contributes to developing students' skills in research, analysis, and technical critique, and prepares them to address contemporary challenges in the cybersecurity domain.

40544109 Intrusion Detection and Prevention, (3) Credit Hours, Prerequisite: 40543204 Network Management and Security, Face-to-Face

This course aims to provide students with the theoretical and practical foundations of concepts and techniques for intrusion detection and prevention in networks and systems. It covers the study of types and patterns of cyber attacks, as well as the design and operation of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), both host-based and network-based. The course also addresses techniques for log analysis and network traffic analysis and their use in tracking abnormal behaviors.

In addition, the course focuses on configuring, tuning, and monitoring these systems in realistic, lab-based environments, while introducing the principles of integration with Security Information and Event Management (SIEM) systems and the role of these technologies in supporting information security policies and incident response. The course includes an applied project or a research-based assignment that enables students to employ the studied tools and techniques in practical scenarios related to intrusion detection and prevention.



40544219 Database Management Systems Security, (3) Credit Hours, Prerequisite: 40742202 Database, Blended.

This course aims to provide students with advanced concepts in the design, development, architecture, and applications of databases, with a particular focus on security challenges across different types of systems. The course includes an in-depth study of SQL, covering topics such as views, exit, with, create type, authorization, metadata, dynamic SQL, triggers, and recursive queries. It also addresses security-related issues such as the data dictionary, normalization and securing relations according to 1NF, 2NF, 3NF, and BCNF, in addition to an in-depth discussion of modern data systems, including object-oriented, distributed, and centralized databases, with an introduction to concurrency control.

The course includes an applied project or research-based assignment through which students employ the theoretical concepts and techniques studied to address practical or research problems in the field of databases and their security.

40544221 Artificial Intelligent Applications in Cybersecurity, (3) Credit Hours, Prerequisite: 40713104 Algorithms Design and Analysis, Blended.

This course aims to introduce students to artificial intelligence (AI) techniques, with a focus on the applications of machine learning and deep learning in computer and network security, software security, and digital forensics. The course includes hands-on programming exercises to apply machine learning and deep learning algorithms for intrusion detection, strengthening network defenses, and enhancing software security, in addition to advanced digital forensics methods for evidence collection and analysis.

Main topics include intelligent intrusion detection systems, biometric security, AI-assisted software vulnerability detection, and code obfuscation. The course also includes an applied project or a research study that enables students to employ these concepts in practical applications or research-oriented studies.

40544220 Emerging Topics on Cybersecurity, (3) Credit Hours, Prerequisite: Complete 60 CH, Blended.

This course aims to familiarize students with the latest developments and emerging issues in the field of cybersecurity, with a focus on advanced threats, innovative solutions, and cutting-edge technologies. The course covers selected topics that evolve in accordance with global challenges and recent developments, enabling students to gain an in-depth understanding of contemporary cybersecurity problems and to address them effectively.

Potential main topics include: advanced cyber attacks, security in cloud environments, machine learning in cybersecurity, advanced cryptography, cybersecurity in industrial control systems, and social engineering.

50521101 Calculus(I), (3) Credit Hours, Prerequisite: -, Blended.

General review of the principles of analytical geometry: the line, the circle, inequalities; functions: their concept, properties, types; limits: definition, concept of one-sided limits, some theorems; continuity: properties and theorems; derivatives: definition, rules, chain rule, higher derivatives, implicit differentiation; applications of differentiation: mean value theorem, increasing and decreasing functions, extreme values, concavity and inflection, horizontal and vertical asymptotes; integration: antiderivative, fundamental theorem of calculus, some applications



of integration, substitution, integration by parts; logarithmic and exponential functions: properties, derivatives, integrals; rational and trigonometric functions: inverses, derivatives, integrals.

50531100 Principles of Statistics and Probability, (3) Credit Hours, Prerequisite: -, Blended.

Describing Statistical Data by tables, graphs and numerical Measures, Measures of Central Tendency and Deviation, counting methods, The Variance, binomial and Normal distribution, probabilities Laws, Random Variables, Sampling distributions, testing of statistical hypotheses for two populations, correlation and regression, correlation coefficient.

50212104 Linear Algebra I, (3) Credit Hours, Prerequisite: 50521101 Calculus, Blended.

Introduction to numerical analysis, and its primary objective is to develop the basic understanding of numerical algorithms and the required skills to implement algorithms to solve mathematical problems, the course includes completing a practical project or research by the students.