جامعــة الـزيتـونـــة الأردنيـة

Al–Zaytoonah University of Jordan

كلية العلوم وتكنولوجيا المعلومات

Faculty of Science and Information Technology

" عراقة وجودة"
"Tradition and Quality"

Brief course description- Course Plan Development and Updating Procedures\ Cybersecurity Department	**QF01/0409-3.0E**

Faculty	Faculty of Science and Information Technology	**Academic Department**	Cybersecurity	Number of The Course Plan (2024-2025\1)
Number of Major Requirement Courses	34	**Date of Plan Approval**	**2024/09/25**	

This form is just for the major requirement courses

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133103	3	Principles of Cybersecurity and Information Security	Fundamentals of Information Technology

The Principles of Cybersecurity and information security course provides a foundational understanding of cybersecurity concepts, emphasizing the distinction between cybersecurity and information security, key threats, and strategies for securing systems and networks. Students will explore topics such as cybercrime, security challenges, and techniques for hardening personal computers and small networks. This course combines theoretical knowledge and practical skills to prepare students to address cybersecurity threats and enhance system resilience.

Course Number	**Credit Hours**	**Title of the Course**	**Prerequisite-Co-Requisite**
0133111	**3**	**Computer Networks**	**Fundamentals of Information Technology**

Introduction to computer networks (goals and applications), Networks Classification, Multiplexing, Network Performance Delay and Loss in Packet-Switched Networks, Application Layer, Principles of Application-Layer Protocols, The World Wide Web: HTTP, Internet's Directory Service: DNS, transport layer services, multiplexing and Demultiplexing application, UDP, TCP, Principles of Congestion Control. The network layer, routing principles, I.P., IPv4, ICMP. Datalink layer services, error detection and correction techniques, sliding window protocols, Multiple Access protocol and LANs, Link layer addressing and address resolution protocol ARP and local area network. it aims of this course is to cover essential Network protocols: ARP, IP, ICMP, IGMP, UDP, TCP, routing protocols such as RIP, OSPF and BGP, multicasting and multicast routing protocols such as DVMRP, MOSPF and PIM, application protocols such as DNS, DHCP, FTP and HTTP. In addition, this course will cover network security protocols such as: https, SFTP, IPSec, VPNs, TLS, SSL, SSH, Kerberos, OSPF authentication and SNMPv3.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133232	3	**Web Application Programming (1)**	Computer Programming

This course provides the students with important components of HTML5, teaching students how to add images, hyperlinks, lists, video, audio and forms to web pages. Further, this course provides an overview of CSS3 and JavaScript, which facilitate disciplined approach to designing computer programs that enhance the functionality and appearance of Web pages.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133212	3	Data Structures and Algorithms	Applied Programming

This course introduces the fundamental concepts of data structures and algorithms using the C++ programming language. Topics include linear and nonlinear data structures such as arrays, linked lists, stacks, queues, trees, and graphs. The course also covers the design and analysis of essential algorithms like sorting, searching, and divide-and-conquer techniques. Emphasis is placed on practical applications to improve programming efficiency and performance.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133220	3	Network Security	Computer Networks

Network security is a critical component of information technology, ensuring the confidentiality, integrity, and availability of data in networked systems. This course provides an in-depth exploration of the principles, techniques, and best practices for securing computer networks against various threats and vulnerabilities. Students will gain a comprehensive understanding of the key concepts, tools, and methodologies used in network security and be prepared to design, implement, and manage secure network infrastructures.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133213	3	امن البنية التحتية باستخدام لينكس Infrastructure Security Using Linux	Applied Programming

The students will have knowledge in underlying operating systems environments such as Linux and Windows and how they contribute, as hosts, to the success of many other applications like network operations and data centers. Students will gain the skills needed to protect Unix and Linux servers from various types of threats. They will learn how to manage users, groups, permissions, ownership, storage, files, directories, Linux boot process, system components, devices, networking, packages, and software.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133333	3	Programming for Cybersecurity	Infrastructure Security Using Linux أمن البنية التحتية باستخدام لينكس

In this course, the basic and advanced concepts in Python language are introduced to write python scripts using variables, conditional statements, strings, methods, lists, tuples dictionary, etc. Additionally, it provides a basic introduction to some security libraries

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133314	3	Operating Systems	0133111

This course connect all computer architecture topics together, and help students to understand how properly the Oss are working. This course introduce the Operating System and Machine Architecture. Operating system and its instruction, the services provided by the OS, process management and its scheduling to the processor, type of scheduling and its algorithms, scheduling criteria's, the modern methods of design and implementation of OS, threads and its models and implementation, deadlock, type of algorithms for prevents the deadlock, manipulation with files, access to the files, the proper storage media for files, memory management, RAM, and VIRUAL memory, paging.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125334	**3**	**Software Security**	0125232, 0133204

The Software Security course provides students with a comprehensive overview of the Software Development Life Cycle (SDLC) from a security perspective. It covers the various phases of the SDLC, emphasizing key security aspects, countermeasures, considerations, and industry standards essential for secure software development.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133222	**3**	**Cryptography theory**	Principles of Cybersecurity and Information Security

This course offers a comprehensive introduction to information security and cryptography, emphasizing their critical role in modern computing. It begins with an exploration of classical encryption techniques, including substitution, transposition, and product ciphers, providing a detailed understanding of conventional encryption algorithms and their design principles. Particular attention is given to symmetric encryption, focusing on widely adopted algorithms such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), alongside stream encryption techniques.Modern cryptographic methodologies are also a key focus, with in-depth coverage of RSA encryption, RSA digital signatures (RSADS), and Diffie-Hellman (DH) secure key exchange. The course further examines the essential topic of pseudorandom number generation and provides an extensive survey of public-key encryption algorithms, highlighting RSA as a cornerstone of modern cryptography. In addition to these foundational topics, the course introduces students to advanced techniques such as digital watermarking and steganography, offering insights into their practical applications in data security and information concealment. By combining theoretical knowledge with practical examples, this course equips students with the skills and understanding needed to navigate and contribute to the evolving field of cryptography and information security.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133204	**3**	**Software Development Life Cycle**	**Emerging Topics in Information Technology**

The "Software Development Life Cycle" (SDLC) course covers software development methods and processes in detail. Students will study SDLC planning, analysis, design, implementation, testing, deployment, and maintenance. Software development is iterative and user requirements are stressed in the training. Students will learn project management and quality assurance methodologies using real-world case studies and best practices. The course also covers Agile and DevOps approaches to prepare students for modern software development difficulties. Software engineering occupations require practical skills learnt through hands-on projects and teamwork.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133205	**3**	**قواعد البيانات وأمنها** **Database and Security**	**Applied Programming**

Database Management Systems (DBMS) describes a standard set of models, design paradigms and a Structured Query Language (SQL). In this background, the course would examine data structures, file organizations, concepts and principles of DBMS's, data analysis, database design, data modelling, database management, data & query optimization, and database implementation. More specifically, the course introduces relational data models; entity-relationship modelling, SQL, data normalization, and database design. It would also introduce query coding practices using MySQL (or any other open system) through various assignments. Design of simple multi-tier client/server architectures based and Web-based database applications will also be introduced. This course also introduces the principles, practices, procedures, and methodologies to ensure the security of data at rest within databases. This course and it appraises the convergence between database security and associated threat vectors/attack methods.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133234	**3**	**Internet Application Programming (2)**	**Internet Application Programming (1)**

Explore the fundamentals of ASP.NET Core MVC in this intensive short course. Designed for beginners, this hands on program covers the essentials of building dynamic, data-driven web applications. Dive into the Model-View Controller architecture, master Razor syntax for views, and understand how to connect your application to databases using Entity Framework Core. Gain practical experience in creating responsive web interfaces and implementing secure authentication. By the end of this course, you'll have the skills to develop robust, interactive web applications with ASP.NET Core MVC.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133223	**3**	**السلامة و المصادقة للبيانات** **Data integrity and authentication**	**Cryptography**

This Course provides knowledge of data integrity and authentication techniques. The following topics must be included in this Course: Authentication Strength, Password Attack Techniques, Password Storage Techniques: Cryptographic Hash Functions, Collision Resistance, Salting, and Data integrity: Message Authentication Codes(MAC), (HMAC), Digital Signatures

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133324	3	**Network Monitoring and Documentation**	Network Security

This course covers standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed local area networks (LANs) and interconnecting T-1/E-1 and T-2/E-3 lines from a central site. The course emphasizes "learning by doing", and requires students to conduct a series of lab exercises. Through these labs, students can enhance their understanding of the principles, and be able to apply those principles to solve real problems.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133325	3	Data Analytics	Data Structures and Algorithms

The course entails a scientific examination of data analytics in the field of cybersecurity, with a particular focus on its application in cybercrime investigations. It provides an overview of cybercrime types and the challenges faced by investigators, emphasizing the importance of digital evidence collection. The course also details the roles and responsibilities of forensic investigators. In addition, this course highlights the centrality of operating systems in cybercrimes and instructs students on the collection and analysis of both volatile and non-volatile data in Windows systems, including memory and registry analysis, browser history examination, and the analysis of Windows OS files, metadata, and logs.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133306	3	Ethical Hacking in Cyber Security	Programming for Cybersecurity

This course equips students with essential knowledge to enhance their ability to detect hacking threats and employ techniques/tools to mitigate them. It covers foundational concepts of hacking, methods for gathering information, target enumeration, port scanning, vulnerability assessment, basics of Windows exploit development, and wireless/web hacking. Additionally, students will learn how to write official penetration testing reports, ensuring clear and professional documentation of findings and recommendations. The course also emphasizes ethical considerations in hacking, highlighting the importance of adhering to legal and moral standards, as well as the critical role of Non-Disclosure Agreements (NDAs) in maintaining confidentiality and trust. Students are strongly advised to avoid practicing any hacking exercises in open or public network environments.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133326	3	Secure Communication Protocols	Network Security أمن الشبكات

In the rapidly evolving of digital communication, the need for robust and reliable security measures has become paramount. The Secure Communication Protocols course provides a comprehensive exploration of contemporary security protocols, their inherent properties, and their practical application. This course covers a wide spectrum of essential topics about the theoretical foundations and practical implementation of secure communication protocols. In addition, the knowledge and skills necessary to design, evaluate, and implement secure communication solutions, contributing to the protection of sensitive data and the integrity of digital interactions.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite

0125349	**3**	**Digital Forensic**	**0125248**

Modern digital systems rely heavily on web applications and IT networks, which are often prime targets for cybercrimes. This course explores web application forensics, addressing the challenges of investigating web-based attacks and analyzing web server logs (IIS). Given that most web applications utilize SQL databases, the course also covers digital forensics for SQL databases, focusing on tracking hacker activities and identifying changes. Additionally, it provides an in-depth understanding of network forensics, highlighting the critical role of network analysis and logging. Students will learn to analyze logs from Routers, Firewalls, IDS, and DHCP systems while documenting network evidence effectively.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133407	**3**	**Practical Malware Analysis**	**Data Safety and Authentication**

This course aims to develop skills for analyzing malicious software using practical tools and techniques. Topics include static and dynamic malware analysis, understanding malware behavior, identifying security threats, and analyzing network traffic. The course emphasizes tools such as disassemblers, debuggers, and virtual analysis environments. It equips students with hands-on experience in threat detection and understanding malware tactics.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133308	**3**	**Cybersecurity Tools and Techniques**	**Programming for Cybersecurity**

This course introduces students to the tools and techniques used in securing systems, networks, and information. Core topics include threat analysis, vulnerability management, penetration testing, and intrusion detection and prevention systems. The course emphasizes practical use of tools such as Wireshark, Metasploit, and Nmap, alongside encryption techniques and firewalls. It aims to develop students' skills in risk assessment and strengthening cybersecurity defenses.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133328	**3**	**Artificial Intelligence in Cybersecurity** ا	**Data Analytics** **تحليلات البيانات**

The course aims to explore fundamental techniques of artificial intelligence (AI) and machine learning (ML) and its role in cybersecurity. Students will implement different AI and ML techniques to detect threats, identify anomalies in networks, prevent cyberattacks in order to improve cybersecurity.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133315	**3**	**Cloud Computing Security**	**قواعد البيانات وامنها** **Database and**

			security

This course covers cloud computing security principles, including service models, deployment strategies, and the shared responsibility model. Topics include IAM, data encryption, virtualization, network security, compliance, and incident response. Hands-on labs and case studies equip students to design and manage secure cloud solutions.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133495	**3**	**Selected Topics in Cybersecurity 1** موضوعات مختارة في الأمن السيبراني 1	Department Approval **موافقة القسم**

The course explores timely and emerging topics that are relevant to cybersecurity. Topics can be gleaned from current issues, such as cloud computing, digital forensics, compliance, software development, IoT, and other contemporary issues in cybersecurity. Both the management and the technical aspect of each cybersecurity issue will be examined and critically analyzed. Students will be given a chance to formulate strategic responses to resolve these issues or improve the situation. The course is research-oriented

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133496	**3**	**Selected Topics in Cybersecurity 2** موضوعات مختارة في الأمن السيبراني 2	Department Approval **موافقة القسم**

This course focuses on emerging technologies for transforming cybersecurity by introducing innovative solutions alongside new challenges. Integrating Artificial Intelligence (AI) and Machine Learning (ML) enhances automated threat detection and predictive analytics, enabling organizations to respond to cyber threats in real-time. Additionally, Blockchain technology provides secure decentralized data storage, while the rise of Internet of Things (IoT) devices highlights significant vulnerabilities due to increased connectivity. As advancements like 5G networks expand attack surfaces and quantum computing threatens traditional encryption methods, understanding these technologies is essential for developing robust cybersecurity strategies that effectively address contemporary threats.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133409		**Security Operations Center (SOC)**	

The Security Operations Center (SOC) Course equips students with the skills to detect, analyze, and respond to cyber threats using industry-standard tools like SIEM, IDS/IPS, and SOAR. Through hands-on labs and real-world simulations, students learn threat hunting, incident response, and the role of automation in cybersecurity. The course emphasizes teamwork, communication, and ethical practices, preparing students for careers in SOC operations. By the end, students will be proficient in managing cyber threats and operating effectively in a SOC environment.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133429	**3**		Data Analytics

		Cybersecurity Governance and Risk Compliance حوكمة الأمن السيبراني والامتثال للمخاطر	تحليلات البيانات

This course focuses on the development and maintenance of effective cybersecurity strategies in n the modern digital landscape. Students will examine key governance measures, risk management strategies, and decision-making frameworks that help organizations manage risk and ensure compliance with industry regulations. Emphasizing the importance of threat-informed decisions, the course covers various risk management approaches and provides insights into the regulatory environment and compliance frameworks commonly adopted to enhance organizational cybersecurity posture. Key areas of focus include governance structures, policies, and procedures that ensure ongoing compliance with legal, ethical, and industry-specific standards. Students will also gain a deeper understanding of how organizations can align their cybersecurity strategies with global regulations such as GDPR, HIPAA, and NIST frameworks. Through practical examples from industry and government, students will learn how robust governance and compliance measures can protect organizations from threats while meeting their compliance obligations across different sectors

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133416	**3**	**Operating Systems' Security**	**0133111**

This course covers both the fundamentals and advanced topics in operating system security. Memory protection and inter-process communications mechanisms will be studied. Students will learn the current state-of-the-art OS-level mechanisms and policies designed to help protect systems against sophisticated attacks. Besides, advanced persistent threats, including rootkits and malware, as well as various protection mechanisms designed to thwart these types of malicious activities, will be studied. Students will learn both hardware and software mechanisms designed to protect the O.S. The course will use virtual machines to study traditional O.S. environments on modern 64-bit systems (e.g., Windows, Linux, and macOS), as well as modern mobile operating systems (e.g., iOS and Android).

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
Secure Communication Protocols	3	**Internet of Things Security**	0133417

This course aims to introduce students to the fundamental concepts of Internet of Things (IoT) security and its challenges. It covers the architecture of IoT systems, common vulnerabilities, secure design techniques, and the use of encryption to protect data. The course also focuses on studying practical case studies for implementing security in IoT environments, providing practical solutions and strategies to mitigate threats. The course is delivered through theoretical lectures and practical sessions to develop students' skills in securing devices and systems.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133102	**3**	**موضوعات حديثه في تكنولوجيا المعلومات**	**اساسيات تكنولوجيا المعلومات**

		Emerging Topics in Information Technology	

This course explores modern topics in information technology, including foundational principles of cybersecurity and artificial intelligence. It emphasizes emerging trends and their implications for the field of IT. Students will gain hands-on experience with basic tools and frameworks to analyze contemporary IT challenges.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133492	**3**	Graduation Project 1 مشروع تخرج 1	Department Approval **موافقة القسم**

This course is the first of two courses that focus on the graduation project. In this course, students prepare a comprehensive proposal for their graduation project, as well as prepare the methodology for this project and the project design. The course introduces students to the basics of research projects, provides them with the basic skills for preparing project proposals, and provides an understanding of the concepts of human research, including its types, stages, and related skills.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0133493	**3**	Graduation Project 2 مشروع تخرج 2	Graduation Project 1

This course is the second of two courses dedicated to the graduation project. In this course, students implement the graduation project approved by the College during the previous semester in Graduation Project-1. The course focuses on developing students' essential skills in effective communication and building positive relationships. It also aims to help students master objective scientific research skills and practice the fundamental abilities required for successful collaboration and scientific inquiry.

Approved by Department Council	**Ahmad Alkhatib**	Date of Approval	16/01/2025