| 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 ( ) |
| **Number of Major Requirement Courses** | 27 | **Date of Plan Approval** | | |

This form is just for the major requirement courses

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| **0115135** | **3** | **شبكات الحاسوب وتراسل البيانات**<br>**Computer Networks and Data Transmission** | **Introduction to 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. | | | |
| **Course Number** | **Credit Hours** | **Title of the Course** | **Prerequisite-Co-Requisite** |
| **0115234** | **3** | **أمن المعلومات والأمن السيبراني**<br>**Information Security and Cybersecurity** | **Introduction to Information Technology** |
| This course provides an introduction to Information Security. The focus is on fundamental concepts and models, Malicious software (Malware), Social Engineering Attacks, Application and Network Attacks, Internet, Wireless, and Other Attacks, Physical Security. Securing the Host, Vulnerability Assessment and Mitigating Attacks, Host, Application, and Data Security. | | | |
| **Course Number** | **Credit Hours** | **Title of the Course** | **Prerequisite-Co-Requisite** |
| **0115212** | **3** | **تراكيب البيانات والخوارزميات**<br>**Data Structure and Algorithms** | **Object-Oriented Programming** |
| The Data Structure and Algorithm course sets out the structuring principles, Abstract Data Types (ADT) and Implementations: Lists, Stacks, Queues, Priority Queues, Recursion. Introduction to algorithm analysis. Introduction of search and sort algorithms including Trees and Binary Search Trees, Hashing, and Heaps. In a high-level language (usually Java) the student should implement the user-defined data structures. Student can compare performance-related alternative implementations of data structures. Write programs that use the arrays, records, strings, linked lists, stacks and queues of each of the following data structures. | | | |
| **Course Number** | **Credit Hours** | **Title of the Course** | **Prerequisite-Co-Requisite** |
| **0115333** | **3** | **تحليل و تصميم النظم الآمنة**<br>**Secure System Analysis and Design** | **Databases** |
| This course presents the techniques and tools for the analysis and design of computer information systems. The focus will be on the life-cycle software development (SDLC) stages. It also highlights | | | |

problem definition, facts gathering techniques and sources, analysis of requirements, specifications, modelling design, input and output design; program coding and conversion of systems. Various analysis/design techniques, modelling tools, structured methodologies, and management skills are introduced throughout the development phases. In this course, we will focus on the secure SDLC being a structural concept for security integration at all stages of the software development life-cycle. Ensuring product protection from scratch not only helps to maintain safety quality but also can help minimize the expense of product production and implementation of security control.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0115332 | 3 | ادارة نظم قواعد البيانات وأمنها<br>Database Management Systems and Security | Databases |

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 |
|---|---|---|---|
| 0115436 | 3 | تقنيات إخفاء المعلومات<br>Information Hiding Techniques | Information Security Protocols |

Steganography is a process which involves hiding a message in an appropriate carrier, for example, an image or an audio file. During this course, an introduction to Steganography is introduced. The difference between Steganography and Cryptography is covered. Also, Steganography techniques and the best tools to perform Steganography will be covered. This course will provide information on how we can hide data and discover the hidden ones using a variety of ways under Windows O.S.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125247 | 3 | نظم تشغيل الشبكات<br>Networks Operating Systems | Computer Networks and Data Transmission |

Each Network Operating System must provide operating system support for hardware, run protocols and services, and provide those services or applications for client systems. Beyond these basic services, NOS may offer administration and management utilities, naming and directory services, file and print services, Web services, backup, security, and network routing, as well as serve as the operating system upon which network applications can be installed and run.
This course will give an overview of the operating system in general and some common distributions. In addition to installing, configuring, and maintaining any Linux system, including systems that supply core Internet and cloud infrastructure. Introduce an overview of system administration, network design, and web hosting. Security features also will be introduced in addition to performance analysis. Also, some essential concepts about windows security will be covered and how to manage file and folder permissions.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125244 | 3 | نظرية التشفير<br>Cryptography | Information Security and Cybersecurity |

This course gives an introduction to information security and its importance, understanding classical encryption Techniques: Substitution, Transposition and product Ciphers, Examination of conventional encryption algorithms and design principles including transposition and substitution techniques such as DES, understanding of the modern cryptographic techniques such as RSA, Key distribution, digital signature, identification and authentication, and sharing keys. Provide a basic understanding of Digital watermarking/Steganography. A survey of symmetric encryption, including classical and modern algorithms, are provided. The emphasis is on the two most important algorithms, the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). This course also covers the most crucial stream encryption algorithm, RC4, and the critical topic of pseudorandom number generation—a survey of public-key algorithms, including RSA (Rivest-Shamir-Adelman).

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125248 | 3 | القرصنة الأخلاقية في الأمن السيبراني<br>Ethical Hacking in Cybersecurity | Cryptography |

The students will learn how to scan, test, hack and secure cyber systems—discovering vulnerabilities so that weak points can be fixed—implementing a secure network that prevents security breaches. The topics covered in this course include Trojans and Backdoors, Viruses and Worms, Sniffers, Social Engineering, Phishing, Denial of Service. Ethical Hacking helps the cyber system take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125349 | 3 | تحقيقات الأدلة الرقمية<br>Digital Forensics | Cryptography |

Digital forensics is a type of forensics that deals with recovery and investigation of data in digital devices. Digital forensics studies cyber-attack prevention, planning, detection, response, and investigation with the goals of counteracting cybercrimes, and making the responsible persons/groups accountable. The topics covered in this course include fundamentals of digital forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentation. Consequently, digital forensics is now a significant part of many criminal investigations, and its tools are frequently and increasingly being used by law enforcement agencies.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125342 | 3 | أمن التجارة الالكترونية والجرائم السيبرانية<br>E-commerce Security and Cyber Crimes | Ethical Hacking in Cybersecurity |

The course describes the underlying infrastructure required to perform electronic commerce transactions. The various categories of the e-commerce Web site and different models of payment systems available over the Internet is also described. During this course, students are familiarized with

various stages, producers and considerations related to planning, designing, hosting, and launching the Web site. In the second part of this course, the various legal and security issues involved in e-commerce transactions will be described. The students will be familiarized with various needed methods and techniques to protect systems and make them more secure.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125345 | 3 | بروتوكولات أمن المعلومات<br>Information Security Protocols | Ethical Hacking in Cybersecurity |

This course will cover Cryptographic Data Integrity Algorithms and begins with a survey of cryptographic hash functions. It will then covers two approaches to data integrity that rely on cryptographic hash functions: message authentication codes and digital signatures. For Mutual Trust, the course will cover key management and key distribution topics and then covers user authentication techniques. Finally, Network Security and Internet Security will be explored. The course examines the use of cryptographic algorithms and security protocols to provide security over networks and the Internet. Topics covered include network access control, cloud security, transport-level security, wireless network security, e-mail security, and I.P. security.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125336 | 3 | إدارة وتقييم المخاطر<br>Risk Management and Evaluation | Secure System Analysis and Design |

In this course, students will learn about the comprehensive information security risk management system and its procedures and how to define and model information security risks and will apply both qualitative and quantitative risk assessment approaches. Understanding this structure will help students to express the business implications of perceived information security risks. These skills are essential for any successful professional in the field of information security. Students will be provided with theoretical, scientific and realistic expertise to operationalize risk management in private and government organizations, vulnerabilities and threats, risk detection, risk assessment, prevention, etc.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125441 | 3 | أمن الشبكات السلكية واللاسلكية<br>Wireless and Wired Network Security | Information Security Protocols |

Networks are the primary point of entry to most computer systems. Network security is about preserving the appropriate use of network resources while preventing disallowed use. Network layers (OSI) model, Network Security Protocols and Administering a Secure Network, Wireless Network Security, Attacks on wireless networks, Protection techniques. Basic security protocols in cellular, Security of IEEE 802.11. Vulnerabilities of IEEE 802.11 Security. MAC Address Filtering. SSID Broadcast. Wired Equivalent Privacy (WEP). Wireless Security Solutions, Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), Other Wireless Security Steps.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125443 | 3 | مراقبة الشبكات وتوثيقها<br>Network Monitoring and Documentation | Information Security Protocols |

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 |
|---|---|---|---|
| 0125481 | 3 | تدريب ميداني<br>Practical Training | Department Approval |

Practical training gives students experience in the area of Cybersecurity fields.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125471 | 3 | منهجية بناء مشروع آمن<br>Methodology for Building A Secure System | Department Approval |

In this course, students will study all the fundamental aspects of building a graduation project. They will need to prepare a proposal of the project idea, including necessary information about the project, project background, project objectives, implementation mechanisms and implementation plan, target, and the feasibility study. The student should also defence his/her idea by presenting his/her project proposal.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125472 | 3 | مشروع تخرج<br>Graduate Project | Department Approval |

This course gives the students the chance to demonstrate their intellectual, technical and creative abilities through developing a project in one of the Cybersecurity fields. The Graduation Project challenges students to go beyond the learning that occurs as the result of their prescribed educational program. Students shall complete their projects in areas of concentrated study under the direction and supervision of faculty members. The projects will demonstrate the students' ability to: apply, analyze, synthesize, evaluate information, and communicate significant knowledge and comprehension.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125371 | 3 | أدوات وتقنيات الأمن السيبراني<br>Cybersecurity Tools and Techniques | Introduction to Information Technology |

This course introduces tools and techniques for password cracking test password strength in your operating system, or for auditing one remotely. Students will be able to use different penetration testing tools to discover remote software vulnerabilities. They will also know how to conduct necessary penetration tests on small networks, run spot checks on the exploitability of vulnerabilities, or discover the network or import scan data.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125361 | 3 | البرمجيات الخبيثة<br>Malicious Software (Malware) | Computer Networks and Data Transmission |

After completion of this course, the student should know about these topics: What is Malware? What is Malware? Types of Malware, Setup Open-Source Malware Analysis Lab. Tools and Techniques, Basic and Dynamic Analysis. Debugging and Reverse Engineering. Malware Analysis Primer, Basic Static Techniques, Malware Analysis in Virtual Machines, Basic Dynamic Analysis, Malware Behavior, Covert Malware Launching, Malware-Focused Network Signatures.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| 0125362 | 3 | موضوعات مختارة في الأمن السيبراني<br>Selected Topics in Cybersecurity | Department Approval |
| Advanced topics in Cybersecurity prepared by faculty staff and with department approval. | | | |
| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
| 0125325 | 3 | البرمجة بلغة بايثون للأمن السيبراني<br>Python for Cybersecurity | Web Application Programming |
| The student will start with an overview of Python, including how to create and run scripts, use threads, and handle exceptions. After that, a student will learn how to network, including how to use the Python libraries for network scripting and develop basic scripts with network functionality. This course will also cover HTTP programming, security scripting, and forensic scripting. Finally, the student will learn about Twisted Python, including the Echo server and HTTP client. Once the student has completed the course, he/she will be fully capable of debugging and security testing using Python, as well as writing Python scripts. Working files are included. | | | |
| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
| 0125463 | 3 | الذكاء الاصطناعي في الأمن السيبراني<br>Artificial Intelligence in Cybersecurity | Database Management Systems and Security |
| Students will learn about log collection and management (Logs, Syslog, sysmon, The rule-based approach to spotting anomalies), preparing the data for machine learning (techniques for labelling and cleaning the data), typical machine learning techniques and tools (supervised learning, unsupervised learning, deep learning, and large scale data analysis), and other A.I. areas relevant to Cybersecurity such as computer vision and A.I. planning. | | | |
| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
| 0125464 | 1 | التحكم بالوصول للمعلومات والمصادقة<br>Access Control and Authentication | Secure System Analysis and Design |
| This course will define the components of access control, provides a framework for implementation, and discusses legal requirements that impact access control programs, Access Control Policies, Standards, Procedures, and Guidelines Unauthorized Access and Security Breaches. It explores how access controls protect resources against unauthorized viewing, tampering, or destruction and serve as a primary means of ensuring privacy, confidentiality, and prevention of unauthorized access and disclosure. It focuses on access control, such as components, processes, controls, and authentication, as well as security breaches, organizational behavior and social engineering, physical security, remote access control, public key infrastructure and encryption, cryptography, testing, and information assurance. | | | |
| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
| 0125465 | 3 | أمن الحوسبة السحابية<br>Cloud Computing Security | Wireless and Wired Network Security |
| This course focuses on the Cloud Computing Architecture and Security, Current Technologies and Solutions, analyze New and Emerging Cloud Solutions, Identify and Evaluate Cloud Computing | | | |

Architectures, Cloud Architecture Models, Cloud-Based Services, Threats, Components (Logical and Physical), and Security Issues and New Challenges of Cloud Computing.

| Course Number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| **0125466** | **3** | **تقنيات الحماية المتكاملة من الاختراق**<br>**Integrated Penetration Protection Technologies** | **Wireless and Wired Network Security** |

This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as penetration testing and protection, introducing students to penetration testing and vulnerability analysis. It will cover in-depth methodologies, techniques, and tools to identify vulnerabilities, exploit, and assess security risk to networks, operating systems, and applications. The student discovers how system vulnerabilities can be exploited and learn to avoid such problems.

| Course number | Credit Hours | Title of the Course | Prerequisite-Co-Requisite |
|---|---|---|---|
| **0125467** | **3** | **أمن أنظمة التشغيل**<br>**Operating Systems' Security** | **Cloud Computing Security** |

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).

| Approved by Department Council | **Dr Khulood Abu Maria** | Date of Approval | 10/06/2020 |
|---|---|---|---|