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 (2021-2020\19)
Number of Major Requirement Courses	30	**Date of Plan Approval**	2021\7\28	

This form is just for the major requirement courses

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125130	**3**	**مقدمة في تكنولوجيا المعلومات** **Introduction to Information Technology**	**Remedial Computer Skills**
This course aims to give an introduction of Information technology and its applications, the internet, world wide web and different internet threats. Moreover, software types and their uses, computer hardware including input and output devices and communications, networks and cyber threats are also introduced. Finally, an introduction to problem solving using pseudo code and flowcharts are presented in this course.			
Course Number	**Credit Hours**	**Title of the Course**	**Prerequisite-Co-Requisite**
0125220	**3**	**برمجة تطبيقات الإنترنت** **Internet Application Programming**	**Principles of 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**
0125131	**3**	**شبكات الحاسوب (1)** **Computer Networks (1)**	**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**
0125231	**3**	**مبادئ الامن السيبراني** **Principles of Cybersecurity**	**Introduction to Information Technology**
It establishes the knowledge required of any cybersecurity, the students will learn the foundations of threat, attacks & vulnerabilities, detect various types of compromise and have an understanding of			

penetration testing and vulnerability scanning concepts, compare and contrast Information Security roles, explain threat actor types, compare and contrast social engineering attack types topic, determine Malware Types, Assessing Security Posture with Software Tools

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125312	3	تراكيب البيانات والخوارزميات 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
0125233	3	امن البنية التحتية باستخدام لينكس Infrastructure Security Using Linux	Computer Networks (1)

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 centres. They will tackle many areas including networking, backup, data restoration, data security, database operations, load balancing, and more.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125241	3	قواعد البيانات وأمنها Database and Security	Object-Oriented 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
0125244	3	نظرية التشفير Cryptography	Principles of 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** **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** **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
0125245	3	**شبكات الحاسوب (2)** **Computer Networks (2)**	**شبكات الحاسوب (1)** **Computer Networks (1)**

The aim 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
0125340	**3**	**تحليلات البيانات** **Data Analytics**	**Database**

This course presents a gentle introduction into the concepts of data analysis, the role of a Data Analyst,

and the tools that are used to perform daily functions. You will gain an understanding of the data ecosystem and the fundamentals of data analysis, such as data gathering or data mining. You will then learn the soft skills that are required to effectively communicate your data to stakeholders, and how mastering these skills can give you the option to become a data driven decision maker.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125347	**3**	**بروتوكولات الاتصالات الامنة** **Secure communication protocols**	**Computer Networks (2)**

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
0125346	**3**	**السلامة و المصادقة للبيانات** **Data integrity and authentication**	**Cryptography**

This course examines policies, methods and mechanisms for securing enterprise and personal data and ensuring data privacy. Topics include data integrity and confidentiality; access control models; secure database architectures; secure transaction processing; information flow, aggregation, and inference controls; auditing; securing data in contemporary (relational, XML and other NO SQL) database systems; data privacy; and legal and ethical issues in data protection. Programming projects are required.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125232	**3**	امن البيانات و المعلومات **Data and information security**	**Principles of Cybersecurity**

Explain data lifecycle stages and discuss related security
issues. Analyze data quality, accessibility and utility. Manage the creation, change, distribution, storage and
termination of data in a secure way. Discuss and explain data ownership, stewardship, management, possession and governance. Illustrate the importance of data classification in cybersecurity.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125334	**3**	**أمن البرمجيات** **software security**	**Data and information security**

Source and Binary Code Analysis, Static and Dynamic Analysis Techniques, Sandboxing, Common Analysis Tools and Methods. Students should be able to:Describe tools and techniques used for software security analysis. Apply software security analysis tools to analyze unknown software

components.

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125435	3	أمن الشبكات 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
0125468	3	السياسات والتشريعات والأخلاقيات في الامن السيبرني Policy, Legal, Ethics and Compliance	Data integrity and authentication

The students will learn how to Discuss issues related to ethics and practices of using technology and cybersecurity. Discussing legislation, regulations, guidelines and major policies in the field of cybersecurity. Recognize important legislative and ethical issues when dealing with data. Explain correct practices in alignment with cybersecurity legislation, controls and standards

Course Number	Credit Hours	Title of the Course	Prerequisite-Co-Requisite
0125443	3	مراقبة الشبكات وتوثيقها 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 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 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 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 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 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 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 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	Credit	Title of the Course	Prerequisite-Co-

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

Number	Hours		Requisite
0125463	3	الذكاء الاصطناعي في الأمن السيبراني 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 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 Cloud Computing Security	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**
0125467	3	أمن أنظمة التشغيل Operating Systems' Security	Operating Systems
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 Farhan AbdulFatth Farhan**	Date of Approval	8/06/2021