Master of Science in Cybersecurity Course Description

Course Title	Credit Hours	Description
Research Methodology	3	This course deals with qualitative and quantitative research, scientific research methods, experimental design, sampling, measurement, and analysis. It also deals with the ethics of scientific research, how to write scientific research and publish in scientific journals, and the components of a research paper. This course provides details on how to write theses, conduct experiments, and write results and reports.
Blockchain	3	This course offers a comprehensive overview of blockchain, including its principles, applications, and challenges. Throughout the course, students will explore the core concepts of blockchain, including decentralized networks, distributed ledger technology, cryptographic protocols, consensus mechanisms, and smart contracts. They will delve into the development of blockchain and gain insights into its evolution and current state. Practical exercises and projects will provide hands-on experience in blockchain development. By the end of the course, students will have a strong understanding of blockchain and the ability to develop and deploy blockchain-based solutions. This course prepares students to actively contribute to the rapidly evolving field of blockchain technology.
Advanced Network Security	3	This course deals with the main issues in data communications, network security, and how to access information. The most important topics that will be covered in this course include security definition, network security, digital signatures, IP security, Secure Socket Layer, intrusion detection, authentication, firewalls, denial of service, spam, Email viruses, phishing, and an overview of the many attacks on networks and the appropriate ways to deal with and prevent them.
Advanced Topics in Ethical Hacking	3	This course highlights ethical hacking tools to develop skills and techniques to identify host and network vulnerabilities. The course also provides an understanding of the scope of penetration testing

		and the responsibilities of conducting such tests following a strict code of ethics. In addition to using a set of modern software tools to perform various penetration testing tasks on service providers, and how to implement appropriate defense mechanisms to mitigate and address specific problems.
Advanced Topics in Cryptology	3	This course introduces the methods and techniques of encryption and decryption. It includes an explanation of public and private keys, protocols, number generators, digital signatures, and other aspects of encryption. In addition, the role that ethics and information privacy play when applying security to public systems and email content is highlighted as well as higher levels of security for corporate owned and classified government information.
Digital Forensics	3	This course covers methods and procedures for locating and recovering damaged or deleted digital data, and accessing tracking information, such as web history, cookies, and cache. It also sheds light on how the attacks originate on the Internet. This course is also concerned with identifying system vulnerabilities, communication ports, and encryption methods. In addition, this course highlights the topic of incident monitoring and response.
Cyber Law and Crimes	3	This course is concerned with the study of laws related to cyberspace. Where the laws and regulations governing the handling and communication of information in cyberspace will be studied. Electronic crimes of all kinds, such as privacy, impersonation, and disavowal, especially crimes related to electronic commerce, will also be studied. The laws governing these crimes, how to analyze them, and the digital evidence associated with them in a legal way will also be studied.
Cybersecurity Risk Management	3	This course contains a detailed review and analysis of the six-step Risk Management Framework using National Institute of Standards and Technology (NIST) (Special Publication) 800-53 that includes security and privacy controls for information systems and organizations. This course includes the process of risk analysis and classification of cyber risks for information systems, and the application of controls to reduce cyber risks for information management. It also provides an in-depth overview of each RMF

		step along the way of the framework as well as the methodology for monitoring IT systems.
Wireless and Mobile Networks Security	3	This course deals with the main issues in wireless security and how to assess security risks in wireless networks. The most important topics that will be covered in this course include the most important tools, trends and techniques for wireless security, familiarity with the preparation of wireless intrusion prevention systems (WISPS) and how to design a network security architecture. This course includes an understanding of WLAN technology and security solutions, identification of authentication technologies such as WPA / WPA2 Personal and Enterprise, an understanding of IEEE 802.11 authentication and key management (AKM), how to apply WLAN security policies and audit practices, how to secure mobile WLAN endpoints and manage And efficient WLAN operation.
Secure Application Development	3	This course explores the concept and process of threat modeling as a key enabler for an effective and appropriate security architecture for software and information assets. Topics in this course include an in-depth review of different types of threats against software. This program also introduces the basics of building secure software that prevents vulnerabilities that hackers can exploit. Topics covered include Buffer Overflow, unvalidated input, race conditions, access control issues, authentication or authorization vulnerabilities, hashing, and other security practices. It also highlights best practices to avoid most vulnerabilities, and security features for many programming languages such as C, C++, C#, Java, Python, PHP, and Ruby.
Intelligent Intrusion Detection Systems	3	This course examines the various methods used to threaten cyber systems such as viruses, spoofing, and denial of service, phishing, spybots, spam, fake websites, and eavesdropping over wireless networks. It also looks at the different ways hacker's access national, corporate or personal data, and the increasing loss of privacy on social networks. This course also introduces advanced techniques and research in intrusion detection and network defense, network traffic analysis, intrusion analysis, machine

		learning techniques for intrusion detection, data mining for intrusion detection, and advanced persistent threats.
Electronic Commerce Security	3	This course focuses on technologies that provide security services for the web. It also provides a set of procedures, practices, and technologies to protect web servers, web users, and the organizations around them. It also discusses, understands, and uses different security technologies for the World Wide Web (WWW) and how to use these technologies to secure WWW applications and electronic commerce applications.
Cybersecurity Governance	3	This course presents information security strategies that support organizational goals and objectives, comply with applicable legal and regulatory requirements, and are implemented through internal policies and controls by providing oversight to mitigate risks. This course also deals with the organizational structure for building IT frameworks, the strategy and technological aspects of IT governance and basic knowledge about managing different types of information. This course presents a study on Internet risks and a study on governance with a focus on both internal control structures and interaction at the board level.
Machine Learning	3	This course introduces machine learning and data mining techniques. This course also focuses on the use of applied methods and software tools to discover hidden patterns or identify anomalies in data generated in modern information technology networks.
Digital Auditing	3	This course contains the theory and best practice in auditing information systems, and sheds light on the role of the auditor of information systems in the development of systems, and how to determine the controls of computer systems. This course also deals with the mechanism of providing the basics for evaluating the processes and products of a software engineering project for compliance with a specific set of standards. Furthermore, this course presents how to provide useful information to anyone who

		needs to provide an independent assessment of compliance with a set of specific processes, standards and requirements.
Advanced Software Engineering		
Software Project Management	3	This course introduces how to build and manage a software project professionally, in addition to how to develop a plan with a schedule for finished products, a tracking system to monitor the project construction process, and risk management assessment.
Cloud Computing	3	
Advanced Topics in Information Technology	3	
Special Topics in Cybersecurity	3	This course deals with technical developments in the field of cybersecurity and the security of computer networks and systems, which are not covered by other courses in the master's program in cybersecurity. Topics may change from year to year based on current trends in the field.
Research Project	3	In this course student make a research in one of cyber security topics.