Program Name: Diploma in Cyber Security
Qualification Level: High Diploma
Department: Information Technology
College: College of Computer and Information Sciences
Institution: Majmaah University

1. Program Mission:

Prepare qualified national graduates with high skills and enough experience to join and engage into labor market of the different fields of Information Technology by providing the graduates with the modern knowledge, advanced skills, and strong moral values to serve the kingdom of Saudi Arabia.

2. Program Goals:

Program educational objectives define the characteristics of our graduates a few years after they have graduated and are employed or undertaking graduate studies The program is structured to produce graduates who:

1. Practice as computing professionals in areas of Cybersecurity with an appropriate combination of fundamental theoretical knowledge and hands-on skills.
2. Enhance their skills in wide aspects of the security of information systems and specialized skills in computer security incidents and crime evidence and master new computing technologies through self-directed professional development or conduct research in Cybersecurity field.
3. Craft their skills for a career path toward leading positions in the Cybersecurity field.

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours
Level 1	DCS 511	Principles of Information Security	Required	N/A	4
	DCS 512	Network and Communication Security	Required	N/A	4
	DCS 513	Operating Systems Security	Required	N/A	4
	DCS 514	Cryptography Fundamentals	Required	N/A	4
Level 2	DCS 521	Information Security Management	Required	IT 501	4
	DCS 522	Secure Software Development	Required	N/A	4
	DCS 523	Ethical Hacking	Required	N/A	4
	DCS 524	Digital Forensics	Required	N/A	4

No.	Course Code	Course Name	Course Description
1	DCS 511	Principles of Information Security	This course is a key component that provides fundamental overview of information security and establishes a solid foundation for the following program courses. The topics cover the following: Information Security Fundamental, Key Information Security Concepts, Characteristics of Information, and Components of an Information System, Balancing Information Security and Access, Risk Analysis, Physical Design, Security Technology Concepts.
2	DCS 512	Communication and Network Security	This course aims to introduce wireless networks, including cellular, fixed wireless access, and wireless LANs, secure networking security attacks, network security practice, email security, IP security, web security, intrusion detection and prevention systems. In this course students will also learn advanced concepts in network security and their implementation in network and how to analyze and assess security of network installations in different setups. Hand on experiments include the execution of attacks, the setup of intrusion detection and prevention, securing computers and wired and wireless networks
3	DCS 513	Operating Systems Security	This course provides students with the theories and tools used to secure common operating systems Linux and Windows. Topics covered include OS security layers, authentication, authorization, and accountability, Security policies, building a secure OS for Linux/Windows
4	DCS 514	Cryptography Fundamentals	This course helps the students to learn cryptographic concepts. In this course students will learn the workings of cryptographic systems and use them in real-world applications. Topics covered include cryptographic primitives such as symmetric encryption, Number Theory, public key encryption, hashing functions, digital signatures, and message authentication

No.	Course Code	Course Name	Course Description
			codes, cryptographic protocols, key establishment, and Electronic commerce.
5	DCS 521	Information Security Management	This course aims to provide the students the knowledge of cybersecurity management, risks involved, and controls used in preventing cybersecurity risks. Students will also learn to implement the control framework in business and Governance. Students will know the methods of security verification and validation. Students will know the various frameworks used in cybersecurity management.
6	DCS 522	Secure Software Development	This course will provide students to understand the theories and tools used for secure software design, threat analysis, secure coding, and vulnerability analysis. Students will study, in-depth, vulnerability classes to understand how to protect software and how to develop secure software. This course will also cover various analysis and design techniques for improving software security.
7	DCS 523	Ethical Hacking	This course aims to provide the students the knowledge of ethical hacking techniques commonly used to breech and exploit corporate networks and to identify how and when they are used. This course teaches penetration testing techniques that quickly, efficiently and most importantly methodically uncover vulnerabilities in operating systems, applications and networks. Students will learn core skills and techniques that every penetration tester needs.
8	DCS 524	Digital Forensics	This course gives the students a solid foundation to the method of computer forensics and investigations. It provides an in-depth knowledge of the criminal justice system, computer hardware and software systems, investigative and evidence gathering protocols. The topics covered will enable the students to possess the knowledge, skills and experience to

No.	Course Code	Course Name	Course Description
			conduct complex, data-intensive forensic examinations involving various operating systems, platforms and file types.