KINGDOM OF SAUDI ARABIA
King Abdutylaziz University
FACULTY OF COMPUTING
& INFORMATION TECHNOLOGY

المملكة العربية السعودية
جامعة الملك عبدالعزيز
كلية الحاسبات
وتقنية المعلومات

Executive Master in Cybersecurity
Coursework and Research Project

Program General Requirements

To obtain a master's degree in cybersecurity, the student must complete at least (30) accredited credits, including the research project, distributed as follow :

- (21) accredited units for compulsory courses
- (6) accredited units for elective courses
- (3) accredited units for the research project

The following are the details of the courses:

a. (21) credit units for compulsory courses:

الوحدات الدراسية	Course Title	اسم المقرر	رمز ورقم المقرر	
			English	عربي
3	Cyber Security Fundamentals	أساسيات الأمن السيبراني	EMCS - 601	م ت أ س – 601
3	Cybersecurity Policies & Issues	سياسات وقضايا الأمن السيبراني	EMCS – 602	م ت أ س – 602
3	Effective Leadership	القيادة الفعالة	EMCS – 603	م ت أ س – 603
3	Information Risk Management	إدارة مخاطر المعلومات	EMCS – 611	م ت أ س – 611
3	Applied Cryptography	التشفير التطبيقي	EMCS – 621	م ت أ س – 621
3	Network Security	أمن الشبكات	EMCS – 631	م ت أ س – 631
3	Network Security	التقييم الأمني	EMCS - 641	م ت أ س – 641

b. (6) credit units for elective courses:

الوحدات الدراسية	Course Title	اسم المقرر	رمز ورقم المقرر	
			English	عربي
3	Digital Forensics	الأدلة الجنائية الرقمية	EMCS – 641	م ت أ س – 642
3	Database Security	أمن قاعدة البيانات	EMCS – 651	م ت أ س – 651
3	Web Security	أمن الويب	EMCS – 652	م ت أ س – 652
3	Cloud Computing Security	أمن الحوسبة السحابية	EMCS – 653	م ت أ س – 653
3	Software Development Security	أمن تطوير البرمجيات	EMCS – 661	م ت أ س – 661
3	Wireless Network Security	أمن الشبكات اللاسلكية	EMCS – 632	م ت أ س – 632
3	Selected Topics in Security	موضوعات مختارة في الأمنية	EMCS - 691	م ت أ س – 691

c. (3) credit units for research project

الوحدات الدراسية	Course Title	اسم المقرر	رمز ورقم المقرر	
			English	عربي
3	Research Project	مشروع بحثي	EMCS - 698	م ت أ س – 698

Courses Description

Course Code	Course Title	Credits	Prerequisite
EMCS-601	Cybersecurity Fundamentals	3	---

This course includes an overview of Cyberspace, defines the scope of Cybersecurity, and addresses information classification and system compartmentalization. The course includes an appreciation of information confidentiality, integrity, and availability, and covers Cybersecurity architecture, strategy, services, and hardware, software, and cloud services. The course also examines national security issues, critical infrastructure, and the potential for cybercrime and cyber terrorism, as well as the need for corporations to align their security with business needs and consider the threat from malicious employees, contractors, and/or vendors.

Course Code	Course Title	Credits	Prerequisite
EMCS-602	Cybersecurity Policies & Issues	3	---

This Course provides a comprehensive examination of the laws, regulations, and Executive Orders concerning privacy, including PCI, HIPAA, GLBA and their overseas counterparts, and the roles of country and local law enforcement. Additionally, the course addresses intellectual property protection (e.g., SOX, FISMA, NIST), security classifications, data location requirements, audits, compliancy assessments, and individual, class-action, and shareholder derivative litigation and liability.

Course Code	Course Title	Credits	Prerequisite
EMCS-603	Effective Leadership	3	---

This course will prepare students to assume greater leadership roles in their organizations by developing and reinforcing critical skills such as persuasive communication, management of change, negotiation, conflict resolution, and ethics.

Course Code	Course Title	Credits	Prerequisite
EMCS-611	Information Risk Management	3	---

This course analyzes the Business continuity and resilience methodologies in the face of a cyberattack. In this course, you will learn how to establish and maintain an information risk management framework in order to guarantee that security and assurance strategies are aligned with business objectives and are consistent with legal and regulatory obligations. This course will provide students with an introduction to the principle of risk management and its three key elements: risk analysis, risk assessment and vulnerability assessment. Students will also learn the differences between quantitative and qualitative risk assessment, and details of how security metrics can be modeled/monitored/controlled and how various types of qualitative risk assessment can be applied to the overall assessment process. Several industry case studies will be studied and discussed. Students will work together in teams to conduct risk assessments based on selected case studies or hypothetical scenarios. Finally, they will write and present their risk assessment reports and findings.

Course Code	Course Title	Credits	Prerequisite
EMCS-621	Applied Cryptography	3	-

This course includes an overview of number theory principles, classic and modern cryptographic methods (symmetric encryption, public key encryption, hash functions, key management, digital signatures, and certificates), electronic mail security, steganography, and recent developments affecting security and privacy on the Internet. The focus will be on how cryptography and its application can maintain privacy and security in electronic communications and computer networks.

Course Code	Course Title	Credits	Prerequisite
EMCS-631	Network Security	3	---

This course provides an in-depth study of network attack techniques and methods to defend against them. Topics include firewalls and virtual private networks; network intrusion detection; denial of service (DoS) and distributed denial-of-service (DDoS) attacks; DoS and DDoS detection and reaction; worm and virus propagation; tracing the source of attacks; traffic analysis; techniques for hiding the source or destination of network traffic; secure routing protocols; protocol scrubbing; and advanced techniques for reacting to network attacks; Digital signatures; Public-Key Infrastructure (PKI) and Trusted Third Party (TTP); Message authentication; Network authentication (Kerberos); Web security protocols such as SSL; Email security protocols; Security in IPv6 networks.

Course Code	Course Title	Credits	Prerequisite
EMCS 632	Wireless Network Security	**3**	--
The course provides an understanding of Security of IEEE 802.11 Wireless LANs; Smart phone and cellular network security; RFID security; Privacy protection in wireless access networks; Location privacy; Anonymous communication in wireless networks; Secure localization; Anti-jamming techniques; Security in cognitive radio networks; Broadcast authentication in wireless sensor networks; Vehicular ad hoc network security.			

Course Code	Course Title	Credits	Prerequisite
EMCS-641	Security Assessment	3	---

The course provides an understanding of the hacking techniques of computers and networks. This course also teaches how to protect Windows and Linux systems. Legal restrictions and ethical guidelines will be taught and enforced. In this course, students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, privilege escalation, Trojans, and backdoors.

Course Code	Course Title	Credits	Prerequisite
EMCS-642	Digital Forensics	3	---

Types of computer crime, Computer misuse, Data protection, Criminal damage, Software piracy, Forgery, Pornography, Unsuitable material, Cybercrime methodologies, Computer forensics investigative theory, Computer forensics processing techniques, File system forensics, Forensics network investigations, Linux for forensics analysis, Linux forensics tools, Forensics investigation on mobile devices.

Course Code	Course Title	Credits	Prerequisite
EMCS-651	Database Security	3	---

This Course provides an introduction to Database Security, Database Authentication, Discretionary Access Control, Role Based Access Control, Mandatory Access Control, Security threats with respect to SQL injections, Database Inference, Virtual Private Databases (VPD), Security in Statistical Databases, Encryption mechanisms in Databases, Database Auditing, Data mining.

Course Code	Course Title	Credits	Prerequisite
EMCS 652	Web Security	3	--

Client-side (browser) vulnerabilities associated with browsing the web, system penetration, information breach and identity threat. Encrypting data stream using SSL, Confidentiality and Integrity of data using third party transaction protocols e.g. SET, PCI DSS Standard, Server-side security: CGI security, server configuration, access control, operating system security, malicious e-mails, web scripts, cookies, web bugs spyware, rogue AV etc.

Course Code	Course Title	Credits	Prerequisite
EMCS-653	Cloud Computing Security	3	---

Modern virtualization technologies coupled with on-demand IT infrastructures have been widely adopted by industry to save capital and operating expenses. But off-premises on-demand infrastructures give rise to new security concerns. This course covers cloud security, addressing known risks and vulnerabilities and focuses on sound architectural design for secure computing. We cover management, governance, audit, legal issues, and meeting regulatory compliance. We also learn how to deploy critical security mechanisms related to secure isolation, application security, data protection, access control, privacy, key management, provisioning, identity and authorization management, high-availability, management, and compliance in a cloud-enabled environment.

Course Code	Course Title	Credits	Prerequisite
EMCS-661	Software Development Security	3	---
Course Code	**Course Title**	**Credits**	**Prerequisite**
EMCS-691	Selected Topics in Security	3	---

This course emphasizes the recent technologies and trends in any field of cybersecurity. The course has to be approved of by the Department before being opened.

Course Code	Course Title	Credits	Prerequisite
EMCS-698	Research Project	3	-

This course will integrate the concepts, skills, insights and experience gained throughout the course into a research project. In this course, students will conduct research and create an independent, comprehensive practical project related to the field of cybersecurity and present their results at the conclusion of the course.