جامعة اليمامة
Al Yamamah University

# College of Engineering

# Master in Cybersecurity (MCS)

# MCS Courses Description

## Core Courses

**CYB511 - Cybersecurity planning and management:** This course aims to familiarize the students with the procedures and processes for Cybersecurity planning and management at the operational, tactical, and strategic levels. The course addresses a range of topics that include senior executives' role in Cybersecurity, Intellectual property protection, managing system updates, and access control. Students will also be introduced to the incident response, business continuity, and disaster recovery procedures.

**CYB512 - Digital forensics and incident management:** This course aims to familiarize the students with basic terminologies in cybercrimes, forensics, response to security incidents, cybercrime investigations and prosecution. Students will understand the role of technology in investigating cybercrimes and conduct digital forensics and analysis. They will learn tools of imaging different types of electronic media and then analyze these images to retrieve the evidence. They will also learn how an organization can set up a security response team, prepare for security incidents and manage these incidents.

**CYB513 - Information assurance architectures and standards:** This course covers the Knowledge of security architectures used to protect Information systems. Topics related to depth defense, intermediary demilitarized zone, proxy servers, TCB subgroups, Institutional and security structures, and design of secure network will be presented. The course also focuses on the standards of information assurance. In this regard, the course details national standards, international regulations and standards (for example NIST), commercial standards (for example PCI/DSS) and open standards (as OWSAP) related to cybersecurity.

**CYB514 - Penetration testing and ethical hacking:** This course aims to provide the students with a good understanding of ethical penetration testing methodologies. Students learn methods for target reconnaissance, host and service enumeration, vulnerability identification and exploitation, and how attackers use access to expand their influence and control. They will also learn the tools to identify vulnerabilities, exploit, and assess security risks to networks, operating systems, and applications. They will use open-source tools for penetration testing and report the results.

**CYB515 - Vulnerability assessment :** This course aims to provide the students with an introduction to the methodologies and software tools for vulnerability assessment. The course places emphasis on the use of these methodologies to demonstrate, document, report on, and provide a clear roadmap for remediation of vulnerabilities. Students learn methods for target reconnaissance, deep packet scan, detect anomalies, cross-comparison, and log file analysis. They will also be introduced to different filtering algorithms and open-source tools to detect and prevent intrusion at the host and network level.

**CYB516 - Advanced cryptography:** This course provides an extensive overview of topics of advanced cryptography. Students will learn, introduction to theory of numbers, introduction to probabilities and statistics, introduction to linear algebra, Elliptic Curve (EC) cryptography, RSA, AES, RSA fundamental, Non-military and non-sensitization algorithms Suite B, Types of cryptography attacks: Differential cryptanalysis, Man in the middle attack, Linear Analysis, Hashing in digital signatures, keys management, Cryptography Classical analysis, Side Attacks: Timing, Energy Consumption, Attacks by analyzing error differencing, Identity based encryption, Digital signatures, Virtual private networks, quantum computing and Cryptography.

**CYB530 - Project - I:** This course allows students to master a specialized field within the broad field of Cybersecurity by carrying a creative, research-oriented work. The research findings must be documented and defended successfully in a viva voce examination. In project-I, students will be introduced to research methodologies and plan, design, and document their proposals.

**CYB531 - Project - II:** This course allows students to master a specialized field within the broad field of Cybersecurity by carrying a creative, research-oriented work. The research findings must be documented and defended successfully in a viva voce examination. In project-II, students will continue working on their proposals by developing implementations or simulations, and experimental evaluations and analysis of their findings.

## Elective Courses

**CYB520 - Selected topics in cybersecurity:** This course goes beyond the fundamentals of Cybersecurity to cover state of the art, emerging and topical aspects related to Cybersecurity. It describes new threats and types of attacks against computers, networks, and systems. This course allows students to update the understanding and analysis of security requirements and define new adapted security policies.

**CYB521 - Software security:** This course discusses how to develop secure programs. It covers the theories and tools used in developing secure software, such as security coding techniques,

security testing, threats and defending source code variabilities, and techniques to verify software design security. The course will also discuss web application security and attacks in addition to operating systems security. Students will be exposed to techniques necessary for developing dependable software systems.

**CYB522 - Cybersecurity policies and procedures:** This course enables the students to define the security goals of an organization and describe the workflows to achieve these goals. The students learn to develop cybersecurity policies and procedures and tailor them to specific industry needs. They will identify different types of security risks in any organization. Students also learn how to survey/ audit an organization from a physical/IT/network security point of view in the light of different standards set by International Standardization Organizations.

**CYB523 - Cloud security:** This course is designed to introduce the students to the basics of cloud security. It will include Evaluate security issues with cloud infrastructure, review the case studies and standard documents on cloud security, cloud computing security guidelines set forth by the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), European Union Agency for Network and Information Security (ENISA), and Cloud Security Alliance (CSA). It will also review reviews security characteristics of leading cloud infrastructure providers and applied deployment scenarios with the internet of things (IoT) and blockchain.

**CYB524 - Security risk analysis:** This course covers principles and concepts of cybersecurity risk analysis and management (cycle and steps). Methodologies for assessing, measuring and analyzing analytical and quantitative cyber risks will be presented. The course covers standards and frameworks for managing cyber risks, cyber risk management processes at several levels in the organization, the economics of mitigating and reducing cyber risks, transfer, acceptance and handling of cyber risks. This course also deals with organizational characteristics that influence the analysis and management of cyber risks in addition to the policies for dealing with cyber risks for technologies and people and entities.

**CYB525 - Cybersecurity design principles:** This course goes beyond traditional security measures by delving into the core principles of secure-by-design. With a focus on constructing cyber systems that are inherently resilient, this course equips students with essential knowledge and skills to create secure, robust, and reliable digital solutions. Through exploration of cutting-edge design strategies and practical application, students will gain insights into integrating security considerations at every stage of development, ensuring that their cyber systems are not only functional but also fortified against the dynamic landscape of cyber threats.