Course Description

Credit Hours	Course Name	Course Code
4	**Information Security Management**	**SEC6641**

This course is intended to present information security from a system and management perspective, including its definition, process, requirements, frameworks, how to integrate information security into the systems design process, and the security management of the information systems lifecycle. This course will cover foundational technical concepts as well as managerial and policy topics such as security policies, standards, and practices; risk analysis; risk assessments; law and compliance related to information security management; governance and strategic planning for security; developing the security program; and security management models and practices.

Credit Hours	Course Name	Course Code
4	**Introduction to Cryptography**	**SEC6651**

This course covers the basic topics in the field of cryptographic algorithms and their applications. This includes the basic Cryptography terminologies, secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their characteristics, signatures, Cipher types together with typical attack methods such as frequency Analysis. Furthermore, the course covers Public Key Infrastructure support for digital signature and encryption and its challenges.

Credit Hours	Course Name	Course Code
4	**Network Security I**	**SEC6611**

The course details the different network security mechanisms used at the different layers of the communication stack. After a review of security properties, it presents cryptographic protocols. Then it details network security protocols including SSL/TLS, IPSec, PGP – S/MIME, SSH and DNSSEC. The security mechanisms to protect access to the radio network are presented through the study of wireless local area networks and mobile cellular networks.

Credit Hours	Course Name	Course Code
4	**Access Control**	**SEC6642**

The Access control foundation course presents the students with the basic fundamental principles of access control models and techniques in addition to secure flow of information. Also, to understand the effectiveness and limitations of these models and techniques. Expose the students to research work and literature review conducted in access control and connect the students to topics related to access control in operating systems, networks, and databases. Finally, Present the students with modern day problems in access control (e.g., Facebook and social media).

Credit Hours	Course Name	Course Code
4	**Network Security 2**	**SEC6612**

This course addresses some of the advanced network security concepts. The topics include the following:

- Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats)
- Network specific threats and attack types (e.g., denial of service, spoofing, sniffing and traffic redirection, Social engineering (e.g., phishing)
- Examples of malware (e.g., viruses, worms, spyware, botnets, Trojan horses or rootkits)
- Man-in-the-Middle, message integrity attacks, routing attacks, and traffic analysis
- Defense mechanisms and countermeasures (e.g., network monitoring, intrusion detection, firewalls, spoofing and DoS protection, honeypots, tracebacks, and Vulnerability analysis)
- Web security model and web application attacks.

Credit Hours	Course Name	Course Code
4	**Operating System Security**	**SEC6643**

This course covers both fundamentals and advanced topics in operating system (OS) security both theoretical and practical. It will study OS level mechanisms and policies in investigating and defending against real-world threats at operating system level. It presents students to techniques used for memory and file system protection, the types of malware and threats, and techniques used to defend against such threats including intrusion detection, virtualization, and disaster recovery. During this course, students will have the opportunity to investigate recent research papers as well as existing industrial technologies developed on the course topics.

Credit Hours	Course Name	Course Code
2	**Industrial Seminar**	**SEC6601**

This course intended to keep the students connected with the professional and academic information security experts. The topics will vary based on the latest trends in the field from industry and research problems. Students will be exposed to real environment and practices as well as open problems in information security.

Credit Hours	Course Name	Course Code

2	Information Security Regulations and Laws	SEC6609

The information Security regulations and laws connect Information security experts to laws and regulations in the kingdom of Saudi Arabia. The students are presented to laws covering a range of topics in both criminal law and laws concerned with commerce.

Credit Hours	Course Name	Course Code
2	**Research Study**	**SEC6602**

The main goal of this course is to write a complete thesis proposal satisfying the theses' requirements and regulations. This research study course is a pre-requisite for registering the master thesis. Initially, students are associated with potential supervisors based on research interests. Then, students are guided by those supervisors towards writing a complete master thesis proposal. This course is conducted as weekly lectures and meetings in which students and supervisors discuss research topics with the aim to write a complete thesis proposal.

Credit Hours	Course Name	Course Code
12	**Thesis**	**SEC6690**

The thesis aims to introduce students to scientific research in the Information Security discipline. The students will explore in depth an area of research and information security by applying the knowledge acquired through the core and elective courses of the program. The main research topics in the Information Security program include problem solving, knowledge representation and reasoning, machine learning, natural language processing, computer vision, constraint-based reasoning, deep learning, data mining and so on. The students are expected to understand the topics of the these, formulate the problematic of the thesis, arise some research questions, study the literature review, analyze the existent solutions, propose strategies, recommendations, and answers to the raised research questions.

Credit Hours	Course Name	Course Code
4	**Cyber Crime & Digital Forensics**	**SEC6605**

This course is designed to introduce students to Cyber Crimes and Digital Forensics on the national and international levels. The course will cover cybercrimes, prevention, understanding the digital forensics profession and investigations, data acquisition, processing crime and incident scenes, recovering graphics files, and digital forensics analysis and validation. Finally, policies, procedures, and cybercrime governance activities will be covered.

Credit Hours	Course Name	Course Code
4	**Cloud Security**	**SEC6616**

The course presents cloud security principles and mechanisms to protect data, applications, and infrastructure. It also explores different threats and vulnerabilities to cloud computing and how to fix and mitigate them. The course covers the fundamentals of the concepts of cloud security, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service.

Credit Hours	Course Name	Course Code
4	**Penetration Testing**	**SEC6618**

This course prepares students to assess and examine security measures of an origination. Students will learn necessary skills to expose vulnerabilities and weaknesses and then suggest proper recommendations. The course covers in-depth methodologies, techniques, and tools to identify vulnerabilities, exploit, and assess security risks to networks, operating systems, and applications. The course goal is to provide knowledge of the successful ethical penetration testing.

Credit Hours	Course Name	Course Code
4	**Database Security**	**SEC6644**

This course covers the different aspects of database security. It provides an overview of the techniques and practices in access control, auditing and failure recovery. It mainly focuses on relational and object-oriented models. The course also focuses on the security issues in database systems and shows how current and future systems shall design to ensure confidentiality, integrity, and availability.

Credit Hours	Course Name	Course Code
4	**Embedded Systems Security**	**SEC6645**

Embedded systems are growing rapidly across various industries. They play vital role in automating and controlling processes, harvesting and analyzing massive data, and taking numerous actions. Securing systems that rely on embedded hardware and application become persistent needs in today's modern interconnected cyber infrastructure. This course provides an overview of security and privacy challenges related to the deployment of IoT solutions using embedded systems that range from microprocessor/microcontroller-based systems, cards/RFIDs/Near Field Communications (NFC), System-On-Chip (SoC) . The students are presented to applications that exploit various embedded system in the era of Internet of Things (IoT). They are also going to examine benefits, threats and attacks when used as assets for Cyber Security. Also, review related standards and security evaluation methodologies for embedded security and consider/compare related technology e.g. TEE, TPM & Android Host Card Emulation (HCE).

Credit Hours	Course Name	Course Code
4	**Software Security**	**SEC6646**

The course details secure design & programming techniques to defend against software vulnerabilities such as buffer overflow and code injection. The course also explores secure software development through the use of secure design, secure coding, program analysis, and advanced testing

Credit Hours	Course Name	Course Code
4	**Privacy and Identity Management**	**SEC6648**

This course aims to provide an overview to identity management and privacy by presenting working definitions of Personal Identifiable Information (PII); identity management and privacy challenges and best practices; and the combined people, processes, policies, and technology required to manage and secure PII

Credit Hours	Course Name	Course Code
4	**Advanced Cryptography**	**SEC6652**

The course introduces advanced topics related to cryptographic algorithms and applications. It starts by briefly scanning historical, stream, and Block ciphers, in addition to number theory concepts and public key cryptography based on integer factorization problem. Then, it presents necessary mathematical background for modern cryptosystems based on the discrete logarithm problem. The course also presents in greater details one of the most advanced cryptosystems, which is Elliptic Curve Cryptography (ECC). Advanced digital signature algorithms such as ECC digital signature and DSA are covered by the course. Moreover, the course presents recent techniques related to the topic of key establishment. Finally, the course introduces recent research directions and the state of the art cryptography-based technologies such as Blockchain and cryptocurrencies, and illustrates the concept of Quantum computing and its impact on cryptography