1. **Course number and name**
   COE444 – Computer Security

2. **Credit and contact hours**
   3 credit hours, 3 contact hours

3. **Instructor's or course coordinator's name:**
   Dr. Fadi Aloul

4. **Textbook, title, author, and year:**
   Wm. Conklin et al, *Principles of Computer Security,* 4th edition, McGraw-Hill, 2015.
   **Other supplemental material**
   None

5. **Specific course information**
   a. **Brief description of content of the course (catalog description)**
      Covers a broad variety of topics in computer security. Includes the following topics: authentication and authorization, introduction and application of cryptography, social engineering attacks, physical security, network security, application security (web, email), wireless security, operating system security, program security, security management, and ethical and legal issues in computer security.

   b. **Prerequisites or co-requisites**
      Prerequisite: COE370 (Communications Networks) or COE371 (Computer Networks I)

   c. **Indicate whether a required, elective, or selected elective course in the program**
      Selected Elective

6. **Specific goals for the course**
   a. **Specific outcomes of instruction**
      This course requires the student to demonstrate the following:
      1. Identify the basic principles of computer security (e.g. confidentiality, integrity, and availability).
      2. Secure operating systems using user authentication and access control.
      3. Describe the threats and countermeasures of physical security and social engineering attacks.
      4. Use cryptography and public key infrastructure to protect data.
      5. Defend against network hacking attacks, including malware, ARP poisoning, spoofing, denial-of-service attacks, and man-in-the-middle attacks.
      6. Develop secure wireless networks.
      7. Analyze different types of firewalls and intrusion detection systems to secure the network.
      8. Explain how to secure email and web applications.
      9. Write safe programs and protect software from malicious code.
      10. Develop security strategies for disaster recovery.
      11. Apply ethical and legal principles in computer security.

**b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course**

This course contributes in a significant way to the accomplishment of the following program outcomes:

| Program outcome | Emphasis in this course |
|---|---|
| (a) an ability to apply knowledge of mathematics, science, and engineering | |
| (b) an ability to design and conduct experiments, as well as to analyze and interpret data | |
| (c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability | ○ |
| (d) an ability to function on multidisciplinary teams | ◑ |
| (e) an ability to identify, formulate, and solve engineering problems | ○ |
| (f) an understanding of professional and ethical responsibility | |
| (g) an ability to communicate effectively | ◑ |
| (h) the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context | |
| (i) a recognition of the need for, and an ability to engage in life-long learning | |
| (j) a knowledge of contemporary issues | ○ |
| (k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice. | ◑ |

Emphasis: ● High; ◑ Medium; ○ Low; Blank – Nothing Specific Expected

**7. Brief list of topics to be covered**

I. Principles of Computer Security
II. Access Control
III. Physical Security and Social Engineering
IV. Cryptography
V. Network Security
VI. Wireless Security
VII. Malware and Denial of Service Attacks
VIII. Email and Web Security
IX. Intrusion Detection Systems and Firewalls
X. Program Security
XI. Security Management
XII. Ethical and Legal Issues in Computer Security