1. **Course Number and Course Title:**

   COE444 – Computer Security

2. **Credit Hours:**

   3-0-3

3. **Prerequisites and/or Co-Requisites:**

   Prerequisite: COE370 (Communications Networks) or COE371 (Computer Networks I)

4. **Name and Contact Information of Instructor:**

   Dr. Fadi Aloul

5. **Course Description (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, e-mail), wireless security, operating system security, intrusion detection systems and firewalls, program security, security management, block chain technologies, and ethical and legal issues in computer security.

6. **Textbook and other Supplemental Material:**

   Textbook:

   - Wm. Conklin et al, *Principles of Computer Security,* 5th edition, McGraw-Hill, 2018.

   Supplemental material:

   - None.

7. **Course Learning Outcomes**

   Upon completion of the course, students will be able to:

   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, public key infrastructure and blockchain technologies 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. Explain how to secure email and web applications.
   8. Analyze different types of firewalls and intrusion detection systems to secure the network.
   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.

8. Teaching and Learning Methodologies:

Methods include lectures, labs, homework, quizzes, exams and class discussions.

9. Course Topics and Schedule:

Topic	**Weeks**
Principles of Computer Security	Week 1
Authentication and Authorization	Week 2
Physical Security and Social Engineering	Week 3
Cryptography	Week 4
Cryptography and Public Key Infrastructure	Week 5
Cryptography and Blockchain technologies	Week 6
Network Security – Fundamentals	Week 7
Network Security – Devices & Remote Access	Week 8
Wireless Security	Week 9
Malware and Denial of Service Attacks	Week 10
Email and Web Security	Week 11
Intrusion Detection Systems and Firewalls	Week 12
Program and OS Security	Week 13
Security Management	Week 14
Ethical and Legal Issues in Computer Security	Week 15
Review	Week 16