**COURSE DESCRIPTION FORM**

**INSTITUTION** \_\_\_\_Computer Science\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

BS CS

**PROGRAM (S) TO BE**

**EVALUATED**

1. **Course Description**

**Objectives:** This course provides a broad overview of the threats to the security of information systems, the responsibilities and basic tools for information security, and the levels of training and expertise needed in organizations to reach and maintain a state of acceptable security. It covers concepts and applications of system and data security. Areas of particular focus include secure network design, implementation and transition issues, and techniques for responding to security breaches.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Course Code** | CSC302 | | | |
| **Course Title** | Information Security | | | |
| **Credit Hours** | 3+0 | | | |
| **Prerequisites by Course(s) and Topics** | None | | | |
| **Assessment Instruments with Weights** (homework, quizzes, midterms, final, programming assignments, lab work, etc.) | Quiz,Assignment, Class Participation/ Presentation/Project =40  Midterm = 20  Final Exam = 40 | | | |
| **Course Coordinator** | Dr. M Malook Rind | | | |
| **URL (if any)** | [malook.rind@smiu.edu.pk](mailto:malook.rind@smiu.edu.pk) | | | |
| **Current Catalog Description** |  | | | |
| **Textbook** (or **Laboratory Manual** for Laboratory Courses) | **Text Book:**  1. Computer Security: Principles and Practice, 5th edition by William Stallings  2. Principles of Information Security, 7th edition by M. Whitman and H. Mattord  3. Comptia Security+ Guide to Network Security Fundamentals 7 Edition by Mark Ciampa  4. The Official (ISC)2 CISSP CBK Reference 6th Edition by Arthur J. Deane, Aaron Kraus  5. Ethical Hacking Essentials (Professional) 1st Edition by EC-Council 2021. | | | |
| **Reference Material** | Latest research papers and white papers | | | |
| **Course Goals/Learning outcomes** | After completing this course, a student will be able to:   * Explain key concepts of information security such as design principles, cryptography, risk management, and ethics. * Discuss legal, ethical, and professional issues in information security. * Apply various security and risk management tools for achieving information security and privacy. * Identify appropriate techniques to tackle and solve problems in the discipline of information security. | | | |
| **Topics Covered in the Course, with Number of Lectures on Each Topic** (assume 15-week instruction and one-hour lectures) | Introduction to Information Security, Threats and Attack Modes, Cryptographic Model, Access Control, Identification and Authentication, Network Security, Operating System (OS) Security Intrusion Detection and Prevention Systems, Privacy Law | | | |
| **Laboratory Projects/Experiments Done in the Course** | NA | | | |
| **Programming Assignments Done in the Course** | NA | | | |
| **Class Time Spent on** (in credit hours) | **Theory** | **Problem Analysis** | **Solution Design** | **Social and Ethical Issues** |
| 38 | 5 | | 5 |
| **Oral and Written Communications** | Every student is required to submit at least Four (4) written assignments, one (1) written report of typically10 - 30 pages and to make one (1) oral presentations of typically 5 -10 minute’s duration. Include only material that is graded for grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy. | | | |

**Instructor Name** \_\_\_Dr. M Malook Rind\_\_\_\_\_\_\_\_

**Instructor Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date** \_18-9-2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Course Log Template**

**Sindh Madressatul Islam University**

**INSTITUTION**

BS (CS)

**PROGRAM (S) TO BE**

**EVALUATED**

|  |  |
| --- | --- |
| **Course Name** | **Information Security** |
| **Catalog Number** | **CSC302** |
| **Instructor Name** | **Dr. Malook Rind** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Duration** | **Topics Covered** | **Evaluation Instruments used** | **Signature** |
| Week 1 | 3 hours | **Course Introduction**  **Information security foundations,**   * The History and Evolution of Information Security * Confidentiality, Integrity, and Availability – The CIA Triad * Threats, Vulnerabilities, and Risks |  |  |
| Week 2 | 3 hours | **Introduction to Information Security**   * The Risk Management Process * The Incident Response Process, Security Control. |  |  |
| Week 3 | 3 hours | **Threats and Attack Modes**   * Threat Terminology, * Types of Attacks; * Spoofing Attacks; * Social Engineering Attacks, |  |  |
| Week 4 | 3 hours | **Threats and Attack Modes**   * Application Attacks; * Web Application Attacks, * Malware attacks, * Denial of Service (DoS) * Distributed Denail of Service (DDoS). | Quiz: 01 |  |
| Week 5 | 3 hours | **Cryptographic Models**   * Cryptographic History, * The Caesar Cipher, * Goals of Cryptography, * Comparing Cryptographic Algorithm, | Assignment:01 |  |
| Week 6 | 3 hours | **Cryptographic Models**   * Symmetric Key Algorithms, * Asymmetric Key Algorithms, * Hashing Algorithms, * Types of Key Algorithms. |  |  |
| Week 7 | 3 hours | **Access Control**   * Access Control Terminology, * Access Control Models. * Mandatory Access Control (MAC) and Discretionary Access Control (DAC) |  |  |
| Week 8 | 3 hours | **Access Control**   * Role-Based Access Control (RBAC) * Rule-Based Access Control (RB-RBAC) |  |  |
| Week 9 | 1.5 hours | Mid Term Examination | |  |
| Week 10 | 3 hours | * **Identification and Authentication** * Identification and Authentication, * Identification, Authentication Types, * Human Authentication Factors, * Authentication Forms, * Authentication Protocols, |  |  |
| Week 11 | 3 hours | **Identification and Authentication**   * Single Sign-On (SSO), * Public-Key Infrastructure (PKI). |  |  |
| Week 12 | 3 hours | **Network Security**   * Network Security Design, * Firewalls, * Network Protection, Web Security.   **Wireless Network Security** | Quiz: 02 |  |
| Week 13 | 3 hours | **Operating System (OS) Security**   * OS Hardening, * OS Protection Methods, * OS Firewalls, OS Security Tools. |  |  |
| Week 13 | 3 hours | **Intrusion Detection and Prevention Systems**   * Intrusion Detection Systems (IDS), * Network Intrusion Detection Systems (NIDS), * Host-based Intrusion Detection Systems (HIDS), * Intrusion Prevention Systems (IPS), * System Information and Event Management (SIEM). | Assignment:02 |  |
| Week 14 | 3 hours | **Privacy Laws, Penalties, and Privacy Issues**   * Electronic Data Privacy Protection, * Global Privacy Laws. |  |  |
| Week 15 | 3 hours | **Ethics in information security** |  |  |
| Week 16 | 3 hours | **Presentations**  **Case studies discussion** |  |  |
| Week 17 | 3 hours | **Revision** |  |  |
| Week 18 | **2 hours** | **Final Examination** | |  |

**Instructor Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date** \_\_\_\_\_\_\_18-9-2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_