|  |  |
| --- | --- |
| **Course Title:** | Cyber Security and Digital Forensic |
| **Course Code:** | **512CCN-3** |
| **Program:** | **Bachelor of Science in Computer Networks** |
| **Department:** | **Department of Computer Networks** |
| **College:** | **College of Computer Science and Information Systems** |
| **Institution:** | **Najran University** |

Table of Contents

[A. Course Identification 3](#_Toc951372)

[6. Mode of Instruction (mark all that apply) 3](#_Toc951373)

[B. Course Objectives and Learning Outcomes 3](#_Toc951374)

[1. Course Description 3](#_Toc951375)

[2. Course Main Objective 3](#_Toc951376)

[3. Course Learning Outcomes 3](#_Toc951377)

[C. Course Content 4](#_Toc951378)

[D. Teaching and Assessment 4](#_Toc951379)

[1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods 4](#_Toc951380)

[2. Assessment Tasks for Students 4](#_Toc951381)

[E. Student Academic Counseling and Support 5](#_Toc951382)

[F. Learning Resources and Facilities 5](#_Toc951383)

[1.Learning Resources 5](#_Toc951384)

[2. Facilities Required 5](#_Toc951385)

[G. Course Quality Evaluation 5](#_Toc951386)

[H. Specification Approval Data 6](#_Toc951387)

# A. Course Identification

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1. Credit hours:** | | | |  | | | | | | | | | | | | |
| **2. Course type** | | | | | | | | | | | | | | | | |
| **a.** | University | |  | | College | | |  | Department | | | |  | Others |  |  |
| **b.** | | Required | | | |  | Elective | | |  |  | | | | | |
| **3. Level/year at which this course is offered:**  **Level 10** | | | | | | | | | | | |  | | | | |
| **4. Pre-requisites for this course** (if any)**:**  411CCN-3 | | | | | | | | | | | | | | | | |
| **5. Co-requisites for this course** (if any)**:** | | | | | | | | | | | | | | | | |
| N/A | | | | | | | | | | | | | | | | |

## 6. Mode of Instruction (mark all that apply)

| **No** | **Mode of Instruction** | **Contact Hours** | **Percentage** |
| --- | --- | --- | --- |
| **1** | **Traditional classroom** | 3 | 100 |
| **2** | **Blended** |  |  |
| **3** | **E-learning** |  |  |
| **4** | **Distance learning** |  |  |
| **5** | **Other** |  |  |

**7. Contact Hours** (based on academic semester)

|  |  |  |
| --- | --- | --- |
| **No** | **Activity** | **Contact Hours** |
| **1** | **Lecture** | 30 |
| **2** | **Laboratory/Studio** | 30 |
| **3** | **Tutorial** | 15 |
| **4** | **Others** (specify) | 45 |
|  | **Total** | 120 |

# B. Course Objectives and Learning Outcomes

|  |
| --- |
| 1. Course Description This course is designed to introduce students to the major discipline of digital forensics and cyber security. It describes describe the role computer forensics and cybersecurity play in deterring and detecting computer crime and in identifying weaknesses and vulnerabilities in computer systems.  The course also introduces the principles of computer forensics, develops the digital forensic analysis knowledge and skills. Students will learn how to respond to cyber breaches, including the recovery, preservation, analysis of digital evidence, and proper incident response. It also discusses prevention, detection, correction and conviction of digital crimes and enhance student of essential knowledge of computing principles such as communication networks and information systems security. |
|  |
| 2. Course Main Objective This course provides students with insight to system forensics investigation and response. It also introduces cybersecurity which includes a comprehensive view of organizational issues involved with privacy, information security, and cybercrime focused on information networks and systems. Areas of study include procedures for investigating computer and cybercrime, and concepts for collecting, analyzing, recovering, and preserving forensic evidence. |
|  |

## 3. Course Learning Outcomes

| **CLOs** | | **Aligned****PLOs** |
| --- | --- | --- |
| 1 | **Knowledge:** |  |
| 1.1 | Define and discuss types of computer crime, intellectual property, and codes of ethics in Information technology professions. | K2 |
| 1.2 | Describe major forensic methodologies | K2 |
|  |  |  |
|  |  |  |
| **2** | **Skills :** |  |
| 2.1 | Analyze potential enterprise security vulnerabilities at various business sectors. | S4 |
| 2.2 | Analyze enterprise security needs and provide recommendations to best suit enterprise technology infrastructure. | S4, S6 |
| 2.3 | Analyze varying forensic approaches to different crimes | S4, S6 |
|  |  |  |
| **3** | **Values:** |  |
| 3.1 | Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. | C3 |
| 3.2 |  |  |
| 3.3 |  |  |
| 3... |  |  |

# C. Course Content

|  |  |  |
| --- | --- | --- |
| **No** | **List of Topics** | **Contact Hours** |
| 1 | Introduction to Digital Forensics and Investigations | 6 |
| 2 | Overview of Computer Crime | 4 |
| 3 | Forensic Methods and Labs | 12 |
| 4 | Collecting, Seizing, and Protecting Evidence | 8 |
| 5 | Techniques for Hiding and Scrambling Information | 5 |
| 6 | Intrusion Detection Strategies | 10 |
| 7 | Enterprise Architecture Security Threats, Prevention, and Recovery | 10 |
| 8 | Security Awareness, Policies, and Digital Crime | 5 |
| ... |  |  |
| **Total** | | 60 |

# D. Teaching and Assessment

## 1. Alignment of Course Learning Outcomes with Teaching Strategies and Assessment Methods

| **Code** | **Course Learning Outcomes** | **Teaching Strategies** | **Assessment Methods** |
| --- | --- | --- | --- |
| **1.0** | **Knowledge** | | |
| 1.1 | Define and discuss types of computer crime, intellectual property, and codes of ethics in Information technology professions. | Lectures, Small Group Work, Small Group Discussion | Quiz 1,Midterm-1 Exam, Final Exam |
| 1.2 | Describe major forensic methodologies | Lectures, Small Group Work, Small Group Discussion | Lectures, Small Group Work, Small Group Discussion |
| … |  |  |  |
| **2.0** | **Skills** | | |
| 2.1 | Analyze potential enterprise security vulnerabilities at various business sectors. | Lectures, Small Group Work, Small Group Discussion | Midterm-1 Exam, Final Exam |
| 2.2 | Analyze enterprise security needs and provide recommendations to best suit enterprise technology infrastructure. | Lectures, Small Group Work, Small Group Discussion | Midterm-1 Exam, Final Exam , Lab Assignment, Lab Final Exam |
| 2.3 | Analyze varying forensic approaches to different crimes | Lectures, Small Group Work | Midterm-2 Exam , Lab Assignment, Lab Final Exam |
| **3.0** | **Values** | | |
| 3.1 | Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles. | Lectures, Small Group Work | Midterm-1 Exam, Final Exam , Lab Assignment, Lab Final Exam, Group Assignment |
| 3.2 |  |  |  |
| … |  |  |  |

## 2. Assessment Tasks for Students

| **#** | **Assessment task\*** | **Week Due** | **Percentage of Total Assessment Score** |
| --- | --- | --- | --- |
| **1** | Quiz and Assignment | 2 | 10 |
| **2** | Midterm Examination 1 | 5 | 15 |
| **3** | Midterm Examination 2 | 9 | 15 |
| **4** | Lab Activities | 8 | 10 |
| **5** | Lab Final Examination | 14 | 10 |
| **6** | Final Examination | 15 | 40 |
| **7** |  |  |  |
| **8** |  |  |  |

**\*Assessment task** (i.e., written test, oral test, oral presentation, group project, essay, etc.)

# E. Student Academic Counseling and Support

|  |
| --- |
| **Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice :** |
| Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)    During the whole semester, 10 hours/week are reserved for students to guide them, to help them, to explain them topic which is not clear to them etc. |

# F. Learning Resources and Facilities

## 1.Learning Resources

|  |  |
| --- | --- |
| **Required Textbooks** | 1. System Forensics, Investigation, and Response, Second Edition, Chuck Easttom: ISBN-13: 978-1-284-03105-8 2. Harwood, M. (2016). Internet Security: How to Defend Against Attackers on the Web (2nd ed.). Burlington, MA: Jones & Bartlett Learning. |
| **Essential References Materials** | 1. Stallings, W., & Brown L. (2015). Computer security: Principles and practice (3rd ed.).. Upper Saddle River, NJ: Pearson Education, Inc. ISBN-13: 9780133773927 |
| **Electronic Materials** | Available in Blackboard |
| **Other Learning Materials** |  |

## 2. Facilities Required

| **Item** | **Resources** |
| --- | --- |
| **Accommodation**  (Classrooms, laboratories, demonstration rooms/labs, etc.) | * Lecture Rooms with 20 seats with smart table, Mic, Speaker, PC, Auto Projector with Screen and a white board or a smart board (male Section). * IoT Lab. |
| **Technology Resources**  (AV, data show, Smart Board, software, etc.) | * Desktop/ Laptop computer Multimedia Projector * Laboratory contains an enough number of PC to accommodate all students with Java-related software like JCreator , J2SE , NetBean, Eclipse and JRE licensed version with network package should be installed. |
| **Other Resources**  (Specify, e.g. if specific laboratory equipment is required, list requirements or attach a list) | A File cabinet to keep class stuffs, papers and students files, and a printer to print program screen shots. |

# G. Course Quality Evaluation

| **Evaluation**  **Areas/Issues** | **Evaluators** | **Evaluation Methods** |
| --- | --- | --- |
| Feedback about Course Learning Outcomes (CLOs) | Students, Faculty | Direct (A course survey is distributed to students to take their opinion) |
| feedback about the teaching strategies, assessment methods, textbooks, instructor | Students | Direct (A course survey is distributed to students to take their opinion) |
| feedback about the teaching strategies, assessment methods, textbooks, instructor | Faculty | Direct (Meeting with course coordinator and college coordinator periodically.) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Evaluation areas** (e.g., Effectiveness of teaching and assessment, Extent of achievement of course learning outcomes, Quality of learning resources, etc.)

**Evaluators** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

**Assessment Methods** (Direct, Indirect)

# H. Specification Approval Data

|  |  |
| --- | --- |
| **Council / Committee** |  |
| **Reference No.** |  |
| **Date** | January 19, 2019 |