هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024
TP-153

# Course Specification
## (Bachelor)

| | |
|---|---|
| **Course Title:** | **Risk management** |
| **Course Code:** | **CYB 0201** |
| **Program:** | **Computer Science( Cybersecurity)** |
| **Department:** | **Applied Science** |
| **College:** | **Applied Collage** |
| **Institution:** | **Imam Muhammad Bin Islamic Universirty** |
| **Version:** | *Course Specification Version Number* |
| **Last Revision Date:** | *Pick Revision Date.* |

## Table of Contents

## A. General information about the course:

### 1. Course Identification

| 1. Credit hours: ( 3(2 Theory, 2 Lab) ) | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| **2. Course type** | | | | | |
| **A.** | ☐University | ☐College | ☒ Department | ☐Track | ☐Others |
| **B.** | ☒ Required | | ☐Elective | | |
| **3. Level/year at which this course is offered: (First Semester)** | | | | | |
| **4. Course General Description:** | | | | | |
| **This course introduces students to the management of information related risks in the area of computer security. Students will learn the knowledge and skills of the models, methodologies and processes for assessing, managing and dealing with cyber risks.** | | | | | |
| **5. Pre-requirements for this course** (if any): | | | | | |
| CYB 0209 ( Operating System Security) | | | | | |
| **6. Co-requisites for this course** (if any): | | | | | |
| None | | | | | |
| **7. Course Main Objective(s):** | | | | | |
| • **Understand risk management fundamentals and classify information and assets**<br>• **Demonstrate an understanding of the concepts of assessment, assets, vulnerabilities, threats, and risks**<br>• **Identify and analyze risks, threats and vulnerabilities impacting an organization**<br>• **Identify and analyze risks, threats and vulnerabilities impacting an organization**<br>• **Explain the difference between Disaster Recovery, and Business Continuity** | | | | | |

### 2. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1 | Traditional classroom | 3 hours\week | 100% |
| 2 | E-learning | | |
| 3 | Hybrid<br>• Traditional classroom<br>• E-learning | | |
| 4 | Distance learning | | |

## 3. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | **Lectures** | 24 |
| 2. | **Laboratory/Studio** | |
| 3. | **Field** | |
| 4. | **Tutorial** | 24 |
| 5. | **Others (specify)** | |
| **Total** | | 48 |

## B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| **1.0** | **Knowledge and understanding** | | | |
| 1.1 | Demonstrate the main risk management methodologies and Relate risk to a cybersecurity policy. | **K1** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| 1.2 | Demonstrate an understanding of the concepts of assessment, vulnerabilities, threats, and risks | **K2** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| 1.3 | Explain correct practices in alignment with cybersecurity legislation, controls and standards | **K3** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| **2.0** | **Skills** | | | |
| 2.1 | Identify and analyze risks, threats and vulnerabilities impacting an organization and identify Relate risk to a cyber-security policy. | **S1** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| 2.2 | Perform a risk assessment and choosing the appropriate methodology | **S2** | Class Discussion Questions/Answers sessions in class | Quizzes, Exams, Project, Presentation |

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| | for dealing with cyber risks | | Case studies and analysis.<br>Project and students | |
| 2.3 | Evaluate and categorize risk with respect to technology, individuals and entities. | **S4** | Class Discussion<br>Questions/Answers sessions in class<br>Case studies and analysis.<br>Project and students | Quizzes, Exams, Project, Presentation |
| **3.0** | **Values, autonomy, and responsibility** | | | |
| | | | | |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | Risk Management Fundamentals. | **4** |
| 2. | -Principles and Concepts of Cyber-security Risk Analysis and Management. | **6** |
| 3. | Risk Management Lifecycle and Steps | **6** |
| 4. | Cyber Risk Assessment and Analysis Methodologies, Methodologies for Measuring and Evaluating Cyber Risk. | **6** |
| 5. | Cyber Risk Management Standards and Frameworks<br>-National and International Cybersecurity Standards and Controls (e.g. Essential Cybersecurity Controls (ECC) issued by the National Cybersecurity Authority, HIPAA, ISO 27001, PCI DSS) | **6** |
| 6. | Cyber Risk Management Processes Across Levels in the Organization and Cyber Risks Acceptance and Mitigation Economics. | **6** |
| 7. | Cyber Risks Policies for Technologies, Individuals and Entities.<br>-Judicial Authorities, Agreements, Treaties and International Organizations Related to Cybersecurity | **6** |
| 8. | Characteristics of Organizations that Influence Cyber Risk Analysis and Management. | **4** |
| 9. | -Communication of Cyber Risks, Accepting and mitigation of Cyber Risks.<br>-Best Practices for Aligning with Cybersecurity Legislation, Controls and Standards | **4** |
| **Total** | | **48** |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | Quizes | 3, 8 | 10% |
| 3. | Midterm | 7 | 20% |
| 4. | Lab Assignments group or individual /Class Assignments group or individual | 4,7,9 | 15% |
| 4. | Lab Evaluations | All Semester | 15% |
| 5. | Project | 10 | 10% |
| 6. | Final | 13, 14 | 30% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

## E. Learning Resources and Facilities

### 1. References and Learning Resources

| | |
|---|---|
| Essential References | The Security Risk Assessment Handbook, A Complete Guide for Performing Security Risk Assessments, Second Edition, By Douglas Landoll · 2016<br>Gibson, D., Igonor, A., 2020, Managing Risk in Information Systems, Jones & Bartlett Learning; 3rd edition |
| Supportive References | Jones, A. and Ashenden, D., 2005. Risk management for computer security. Oxford: Butterworth-Heinemann |
| Electronic Materials | Online resources will be provided during class lectures |
| Other Learning Materials | N/A |

### 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| **facilities**<br>(Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | Lecture room with Smart board Lab with 25 Pcs |
| **Technology equipment**<br>(projector, smart board, software) | PC and WiFi Internet access within the classroom |
| **Other equipment**<br>(depending on the nature of the specialty) | N\A |

## F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Student | Indirect using course evaluation survey |
| Effectiveness of Students assessment | Student | Indirect using course evaluation survey |
| Quality of learning resources | Student and Faculty | Indirect using course evaluation and faculty survey |
| The extent to which CLOs have been achieved | | |
| Other | | |

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

Assessment Methods (Direct, Indirect)

## G. Specification Approval

| | |
|---|---|
| COUNCIL /COMMITTEE | |
| REFERENCE NO. | |
| DATE | |

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024
TP-153

# Course Specification
## (Bachelor)

| | |
|---|---|
| **Course Title:** | Ethical hacking |
| **Course Code:** | CYB 0206 |
| **Program:** | Computer Science( Cybersecurity) |
| **Department:** | Applied Science |
| **College:** | Applied Collage |
| **Institution:** | Imam Muhammad Bin Islamic Universirty |
| **Version:** | *Course Specification Version Number* |
| **Last Revision Date:** | 1445 |

## Table of Contents

## A. General information about the course:

### 1. Course Identification

| 1. Credit hours: ( 4(3 Theory, 2 Lab) ) | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| **2. Course type** | | | | | |
| **A.** | ☐University | ☐College | ☒ Department | ☐Track | ☐Others |
| **B.** | ☒ Required | | ☐Elective | | |
| **3. Level/year at which this course is offered: (First Semester)** | | | | | |
| **4. Course General Description:** | | | | | |
| **This course covers ethical hacking and penetration testing techniques using the latest software, techniques, and methodologies used by hackers and security professionals to lawfully hack an organization. Topics include session hijacking, hacking of web applications and servers, as well as social engineering and denial of services hacking techniques.** | | | | | |
| **5. Pre-requirements for this course** (if any): | | | | | |
| CYB 0202 ( Cyber Threats) | | | | | |
| **6. Co-requisites for this course** (if any): | | | | | |
| None | | | | | |
| **7. Course Main Objective(s):** | | | | | |
| • **Demonstrate an understanding of ethical hacking**<br>• **Identify possible ways to hack web applications**<br>• **Describe several techniques to attack wired and wireless networks**<br>• **Explain the concept of social engineering** | | | | | |

### 2. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1 | Traditional classroom | 4 hours\week | 100% |
| 2 | E-learning | | |
| 3 | Hybrid<br>• Traditional classroom<br>• E-learning | | |
| 4 | Distance learning | | |

## 3. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | **Lectures** | 36 |
| 2. | **Laboratory/Studio** | 24 |
| 3. | **Field** | |
| 4. | **Tutorial** | |
| 5. | **Others (specify)** | |
| **Total** | | 60 |

## B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| **1.0** | **Knowledge and understanding** | | | |
| 1.1 | Demonstrate an understanding of ethical hacking | **K1** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| **2.0** | **Skills** | | | |
| 2.1 | Identify possible ways to hack web applications | **S1** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| 2.2 | Describe several techniques to attack wired and wireless networks | **S2** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| 2.3 | Explain the concept of social engineering | **S3** | Class Discussion Questions/Answers sessions in class Case studies and analysis. Project and students | Quizzes, Exams, Project, Presentation |
| **3.0** | **Values, autonomy, and responsibility** | | | |
| | | | | |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | Introduction to Ethical Hacking and Penetration Testing | 6 |
| 2. | Planning and Scoping a Penetration Testing Assessment | 8 |
| 3. | Information Gathering and Vulnerability Scanning | 10 |
| 4. | Social Engineering Attacks | 10 |
| 5. | Exploiting Wired and Wireless Networks | 10 |
| 6. | Exploiting Application-Based Vulnerabilities | 4 |
| 7. | Cloud, Mobile, and IoT Security | 4 |
| 8. | Performing Post-Exploitation Techniques | 4 |
| 9. | Reporting and Communication | 4 |
| | Total | 60 |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | Quizes | 3, 8 | 10% |
| 3. | Midterm | 7 | 20% |
| 4. | Lab Assignments group or individual /Class Assignments group or individual | 4,7,9 | 15% |
| 4. | Lab Evaluations | All Semester | 15% |
| 5. | Project | 10 | 10% |
| 6. | Final | 13, 14 | 30% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

## E. Learning Resources and Facilities

### 1. References and Learning Resources

| | |
|---|---|
| Essential References | Regalado, D. et al. , "Gray Hat Hacking: The Ethical Hacker's Handbook", 2018, 5th Edition. |
| Supportive References | Wenliang Du, "Computer & Internet Security: A Hands-on Approach", 2019, 2nd edition. |
| Electronic Materials | Online resources will be provided during class lectures. |
| Other Learning Materials | N/A |

## 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| **facilities** (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | Lecture room with Smart board Lab with 25 Pcs |
| **Technology equipment** (projector, smart board, software) | PC and WiFi Internet access within the classroom |
| **Other equipment** (depending on the nature of the specialty) | N\A |

## F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Student | Indirect using course evaluation survey |
| Effectiveness of Students assessment | Student | Indirect using course evaluation survey |
| Quality of learning resources | Student and Faculty | Indirect using course evaluation and faculty survey |
| The extent to which CLOs have been achieved | | |
| Other | | |

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

Assessment Methods (Direct, Indirect)

## G. Specification Approval

| | |
|---|---|
| COUNCIL /COMMITTEE | |
| REFERENCE NO. | |
| DATE | |

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAA

2024
TP-153

# Course Specification
## (Bachelor)

| | |
|---|---|
| **Course Title:** | **Software Security Development** |
| **Course Code:** | **CYB 0207** |
| **Program:** | **Computer Science( Cybersecurity)** |
| **Department:** | **Applied Science** |
| **College:** | **Applied Collage** |
| **Institution:** | **Imam Muhammad Bin Islamic Universirty** |
| **Version:** | *Course Specification Version Number* |
| **Last Revision Date:** | *Pick Revision Date.* |

## Table of Contents

## A. General information about the course:

### 1. Course Identification

| 1. Credit hours: ( 3(2 Theory, 2 Lab) ) | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| **2. Course type** | | | | | |
| **A.** | ☐University | ☐College | ☒ Department | ☐Track | ☐Others |
| **B.** | ☒ Required | | ☐ Elective | | |
| **3. Level/year at which this course is offered: (First Semester)** | | | | | |
| **4. Course General Description:** | | | | | |
| **This course deals with security analysis in software development. Identify and detect vulnerabilities that threaten systems. Topics include risk modeling, defensive and security programming on the Internet, the interaction between usability and trust management, safe usage control, the principle of least privilege, information overflow, check time versus time to access, and other related security issues. Advanced topics in the secure design of computer systems. Security services and models. Determining security requirements for computer systems, designing secure software architectures, and verifying the security of software and computer systems. Types of attack, means of checking the credibility of messages.** | | | | | |
| **5. Pre-requirements for this course** (if any): | | | | | |
| CYB 0101 – Information Security Fundamentals | | | | | |
| **6. Co-requisites for this course** (if any): | | | | | |
| None | | | | | |
| **7. Course Main Objective(s):** | | | | | |
| **Students should be able to understand in deep the software development using different systems, and the matter of the secured system. Also, a clear concept must be clear for them in the design matters for security, foundation, threats, mitigation, and the pattern of the secure development. Furthermore, students should be aware of the implementation of any secure design in analyzing level as a developer.** | | | | | |

### 2. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1 | Traditional classroom | 3 hours\week | 100% |
| 2 | E-learning | | |
| 3 | Hybrid<br>• Traditional classroom<br>• E-learning | | |
| 4 | Distance learning | | |

## 3. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | **Lectures** | 24 |
| 2. | **Laboratory/Studio** | 24 |
| 3. | **Field** | |
| 4. | **Tutorial** | |
| 5. | **Others (specify)** | |
| **Total** | | 48 |

## B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| **1.0** | **Knowledge and understanding** | | | |
| 1.1 | Understand the secured software design. | **K1** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports. |
| 1.2 | Demonstrate the main aspects and of secured deign. | **K2** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports.<br>Study cases. |
| **2.0** | **Skills** | | | |
| 2.1 | Learning about secured design, programming, reviewing, level of codes, or level of flows in design. | **S1** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports.<br>Study cases. |

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 2.2 | Analysis of secured system requirements. | **S2** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports.<br>Study cases. |
| **3.0** | **Values, autonomy, and responsibility** | | | |
| 3.1 | Provide a software secured design for a system. | **V3** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments | Project<br>Writing reports.<br>Study cases. |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | Introduction, Why design matters for security | 4 |
| 2. | Foundation: Core concepts of domain driven design | 4 |
| 3. | Concept: Foundation | 4 |
| 4. | Concept: Threats | 4 |
| 5. | Concept: Mitigation | 4 |
| 6. | Concept: Pattern | 4 |
| 7. | Design: Secure Design | 4 |
| 8. | Design: Security Design Reviews | 6 |
| 9. | Implementation: Secure Programming | 6 |
| 10. | Implementation: Low level coding flaws | 4 |
| 11. | Implementation: Untrusted input | 4 |
| **Total** | | **48** |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | Quizes | 3, 8 | 10% |
| 3. | Midterm | 7 | 20% |
| 4. | Lab Assignments group or individual /Class Assignments group or individual | 4,7,9 | 15% |
| 4. | Lab Evaluations | All Semester | 15% |
| 5. | Project | 10 | 10% |
| 6. | Final | 13, 14 | 30% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

## E. Learning Resources and Facilities

### 1. References and Learning Resources

| | |
|---|---|
| Essential References | Designing Secure Software: A Guide for Developers,2022,By Loren Kohnfelder. |
| Supportive References | N/A |
| Electronic Materials | Online resources will be provided during class lectures. |
| Other Learning Materials | N/A |

### 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| **facilities** (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | Lecture room with Smart board Lab with 25 Pcs |
| **Technology equipment** (projector, smart board, software) | PC and WiFi Internet access within the classroom |
| **Other equipment** (depending on the nature of the specialty) | N\A |

## F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Student | Indirect using course evaluation survey |

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of Students assessment | Student | Indirect using course evaluation survey |
| Quality of learning resources | Student and Faculty | Indirect using course evaluation and faculty survey |
| The extent to which CLOs have been achieved | | |
| Other | | |

**Assessors** (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

**Assessment Methods** (Direct, Indirect)

## G. Specification Approval

| | |
|---|---|
| **COUNCIL /COMMITTEE** | |
| **REFERENCE NO.** | |
| **DATE** | |

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

اعتماد
NCAAA

2024
TP-153

# Course Specification
## (Bachelor)

| | |
|---|---|
| **Course Title:** | **Information Security Management** |
| **Course Code:** | **CYB 0208** |
| **Program:** | **Computer Science( Cybersecurity)** |
| **Department:** | **Applied Science** |
| **College:** | **Applied Collage** |
| **Institution:** | **Imam Muhammad Bin Islamic Universirty** |
| **Version:** | *Course Specification Version Number* |
| **Last Revision Date:** | *Pick Revision Date.* |

## Table of Contents



جامعة الملك عبدالعزيز
١٤٠٥هـ ١٤٠٦هـ
الكلية التطبيقية

## A. General information about the course:

### 1. Course Identification

| 1. Credit hours: ( 3(2 Theory, 2 Lab) ) | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| **2. Course type** | | | | | |
| **A.** | ☐University | ☐College | ☒ Department | ☐Track | ☐Others |
| **B.** | ☐ Required | | ☒ Elective | | |
| **3. Level/year at which this course is offered: (First Semester)** | | | | | |
| **4. Course General Description:** | | | | | |
| **This course provides necessary skills and abilities to design cybersecurity plans and processes for an organization. Through a combination of lectures, case studies, and practical exercises, participants will develop the knowledge and skills necessary to assess, plan, and implement cybersecurity measures within organizational contexts effectively.** | | | | | |
| **5. Pre-requirements for this course** (if any)**:** | | | | | |
| None | | | | | |
| **6. Co-requisites for this course** (if any)**:** | | | | | |
| None | | | | | |
| **7. Course Main Objective(s):** | | | | | |
| **Students should be aware of commercial, personal and sensitive information to keep secure. In today's technology-driven environment, there is an ever-increasing demand for information delivery on various devices in the office, at home and in public places, these principles should be illustrated carefully. This course should show the reflect changes in the IT security landscape and Information Security Management Principles.** | | | | | |

### 2. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1 | Traditional classroom | 3 hours\week | 100% |
| 2 | E-learning | | |
| 3 | Hybrid<br>• Traditional classroom<br>• E-learning | | |
| 4 | Distance learning | | |

## 3. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | **Lectures** | 24 |
| 2. | **Laboratory/Studio** | 24 |
| 3. | **Field** | |
| 4. | **Tutorial** | |
| 5. | **Others (specify)** | |
| **Total** | | 48 |

## B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| **1.0** | **Knowledge and understanding** | | | |
| 1.1 | Understand the information security principles and information risk. | **K1** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports. |
| 1.2 | Demonstrates the information security framework and security life cycle. | **K2** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports. |
| **2.0** | **Skills** | | | |
| 2.1 | Explain the security life cycle and the controlling methods. | **S1** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports.<br>Study cases. |

| Code | Course Learning Outcomes | Code of PLOs aligned with the program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 2.2 | Analyze the security environment and the disaster recovery management. | **S3** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments<br>Quizzes<br>Case studies and Analysis. | Quizzes<br>Homework and Assignments.<br>Written exams (Midterm and final).<br>Writing reports.<br>Study cases. |
| **3.0** | **Values, autonomy, and responsibility** | | | |
| 3.1 | Cooperation, teamwork, and professional ethics. | **V3** | Class lectures<br>Class Discussion<br>Questions/Answers sessions in class<br>Home work assignments | Project<br>Writing reports.<br>Study cases. |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | CH1-Information Security Principles | 4 |
| 2. | CH2-INFORMATION RISK | 4 |
| 3. | CH3-INFORMATION SECURITY FRAMEWORK | 4 |
| 4. | CH4-SECURITY LIFE CYCLES | 8 |
| 5. | CH5-PROCEDURAL AND PEOPLE SECURITY CONTROLS | 8 |
| 6. | CH6-TECHNICAL SECURITY CONTROLS | 8 |
| 7. | CH7-Physical And Environmental Security | 6 |
| 8. | CH8-Disaster Recovery And Business Continuity | 6 |
| **Total** | | **48** |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | Quizes | 3, 8 | 10% |
| 3. | Midterm | 7 | 20% |
| 4. | Lab Assignments group or individual /Class Assignments group or individual | 4,7,9 | 15% |
| 4. | Lab Evaluations | All Semester | 15% |
| 5. | Project | 10 | 10% |
| 6. | Final | 13, 14 | 30% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.).

## E. Learning Resources and Facilities

### 1. References and Learning Resources

| | |
|---|---|
| Essential References | Information Security Management Principles, 2020, 3rd edition, Andy Taylor, David Alexander, Amanda Finch. |
| Supportive References | N/A |
| Electronic Materials | Online resources will be provided during class lectures. |
| Other Learning Materials | N/A |

### 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| **facilities** (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | Lecture room with Smart board Lab with 25 Pcs |
| **Technology equipment** (projector, smart board, software) | PC and WiFi Internet access within the classroom |
| **Other equipment** (depending on the nature of the specialty) | N\A |

## F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Student | Indirect using course evaluation survey |
| Effectiveness of Students assessment | Student | Indirect using course evaluation survey |
| Quality of learning resources | Student and Faculty | Indirect using course evaluation and faculty survey |
| The extent to which CLOs have been achieved | | |
| Other | | |

Assessors (Students, Faculty, Program Leaders, Peer Reviewers, Others (specify)

Assessment Methods (Direct, Indirect)

## G. Specification Approval

| | |
|---|---|
| COUNCIL /COMMITTEE | |
| REFERENCE NO. | |
| DATE | |

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

# Course Specification

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

# Course Specification

| | |
|---|---|
| Course Code: | 0291 عال |
| Program: | Cybersecurity |
| Department: | Applied Sciences |
| College: | Applied College |
| Institution: | Imam Mohammad Bin Saud Islamic University |
| Version: | 1st version |
| Last Revision Date: | 2023/11/15 |

## Table of Contents:

# A. General information about the course:

| Course Identification | | | | | |
|---|---|---|---|---|---|
| **1. Credit hours:** | 2 (1 Theory, 2 lab) | | | | |
| **2. Course type:** | | | | | |
| a. | University ☐ | College ☐ | Department☒ | Track☐ | Others☐ |
| b. | Required ☒ | Elective☐ | | | |
| **3. Level/year at which this course is offered:** 3rd Level | | | | | |
| **4. Course general Description:** | | | | | |

The Graduation Project in Cybersecurity is a capstone course designed to provide students with an opportunity to apply the knowledge and skills acquired throughout their cybersecurity diploma program. Students will work on a substantial project or research topic related to cybersecurity, demonstrating their ability to analyze, design, implement, and evaluate solutions to real-world cybersecurity challenges.

This course conducted under the general guidance of an approved faculty member. The course will allow the student to develop various skills, within a context that students will find relevant and engaging. Towards the end of the semester, the students should submit a project report and give a formal presentation.

**5. Pre-requirements for this course (if any):** N/A

**6. Co- requirements for this course (if any):** N/A

**7. Course Main Objective(s):**

The main objective of this course is to provide students with an opportunity to apply the knowledge and skills acquired throughout their cybersecurity diploma program.

**By the end of the course, students will be able to:**

1. Formulate a comprehensive project proposal that addresses a significant cybersecurity issue or research question.
2. Apply relevant cybersecurity concepts, principles, and techniques to analyze, design, and develop a solution or research methodology.
3. Conduct in-depth research and critically analyze existing literature and practices related to the chosen project topic.
4. Implement and test the proposed solution or research methodology, considering cybersecurity best practices and ethical considerations.
5. Evaluate the effectiveness and impact of the project, considering relevant metrics and criteria.
6. Communicate project findings effectively through written reports and oral presentations.

7. Apply project management fundamentals
8. Demonstrate professionalism, teamwork, and time management skills throughout the project duration. *(become familiar with teamwork :team size of 3 to 5 students)*

## 1. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1. | Traditional classroom | | |
| 2. | E-learning | | |
| 3. | Hybrid<br>• Traditional classroom<br>• E-learning | 36 | 100% |
| 4. | Distance learning | | |

## 2. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | Lectures | 12 |
| 2. | Laboratory/Studio | |
| 3. | Field | |
| 4. | Tutorial | 12 |
| 5. | Others (specify)<br>Seminars: The course emphasises group work, guided by weekly face to face (or online) meetings with the advisor (group project supervisor) | 12 |
| | Total | 36 |

# B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 1.0 | Knowledge and understanding | | | |
| 1.1 | Identify a cybersecurity problem | 5ع ،2ع ،1ع | Lectures, Class Discussions | Tutorials |
| 1.2 | Demonstrate in-depth knowledge and understanding of cybersecurity concepts, principles, and technologies. | 5ع ،2ع ،1ع | | |
| 1.3 | Familiarity with international and national regulations and systems related to cybersecurity. | 4ع ،2ع ،1ع | | |

| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 1.4 | Develop robust project management techniques | ع1، ع2، ع5 | | |
| 2.0 | Skills | | | |
| 2.1 | Apply critical thinking and problem-solving skills to identify and address cybersecurity challenges. | م1، م2، م3 | Seminars Class Discussions | Tutorials |
| 2.2 | Conduct independent research and analysis to propose innovative solutions in cybersecurity. | م1، م2، م3، م4، م7 | | |
| 2.3 | Provide a link to the practical experiences of industry professionals, showcasing the relevance of computer security in real-world scenarios. | م1، م2، م4، م6، م7 | | |
| 2.4 | Deliver plans clearly and concisely orally, visually and in a written form | م1، م2، م6، م7 | | |
| 3.0 | Values, autonomy, and responsibility | | | |
| 3.1 | Collaboration, teamwork, and professional ethics. | ق1 | Class Discussions, Class Activity | Group Project Report |
| 3.2 | Take the responsibility for continuous learning, and self-development. | ق2 | | |
| 3.3 | Effective and efficient time management when applying acquired knowledge and skills. | ق3 | | |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | • **Project Proposal Development:**<br>• Identifying a cybersecurity problem or research question with a clear problem statement, objectives, and methodology.<br>• Conducting a literature review and gap analysis | 8 |

| | | |
|---|---|---|
| | • Conducting a feasibility study and assessing the resources required. | |
| 2. | • **Project Planning and Management:**<br>• Project planning, including defining project milestones, tasks, and deliverables.<br>• Risk assessment and mitigation strategies.<br>• Project scheduling and time management. | 6 |
| 3 | • **Project Implementation and Testing**<br>• Designing and developing the proposed solution or research methodology.<br>• Implementing cybersecurity controls and measures.<br>• Conducting testing, data collection, and analysis.<br>• Iterative development and refinement.<br>• Addressing security, privacy, and quality assurance considerations. | 6 |
| 4 | • **Project Documentation and Reporting:**<br>• Writing technical reports and documentation following industry standards.<br>• Creating project artifacts, such as design documents, user manuals, and system documentation.<br>• Presenting project findings and results effectively | 6 |
| 5 | • **Project Evaluation and Documentation:**<br>• Evaluating the effectiveness and impact of the project.<br>• Assessing project outcomes against predefined metrics and criteria.<br>• Documenting project findings, including lessons learned and recommendations.<br>• Writing a comprehensive project report. | 6 |
| 6 | • **Project Presentation:**<br>• Preparing and delivering a professional oral presentation.<br>• Demonstrating effective communication skills.<br>• Responding to questions and feedback. | 4 |

| | |
|---|---|
| Total | 36 |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | **Quizzes and Assignments** | 2,5,7 | 30% |
| 2. | **Project** | Week 5, 10 | 40% |
| 3. | **Final Exam (Viva-voce)** | 12 | 30% |
| 7 | **Total Marks** | | 100% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

# E. Learning Resources and Facilities

## 1. References and Learning Resources

| | |
|---|---|
| Essential References | N/A |
| Supportive References | N/A |
| Electronic Materials | Online resources will be provided during class lectures on LMS. |
| Other Learning Materials | N/A |

## 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| Facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | classrooms |
| Technology equipment (projector, smart board, software) | Data show, internet, PC |
| Other equipment (depending on the nature of the specialty) | N/A |

# F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Peer references – students. | 1.Questionnaires and referendums approved by the department.<br>2.Peer evaluation of faculty members.<br>3.Review the results of the students' evaluation. |
| Effectiveness of students assessment | Peer references - program leaders - faculty members – students. | 1.Questionnaires and referendums approved by the department.<br>2.Review course descriptions and course reports periodically.<br>3.Peer evaluation and periodic exchange of correction and scrutiny among fellow faculty members. |

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| | | 4.Review samples of students' work. |
| Quality of learning resources | Program leaders - faculty members - students | 1.Questionnaires and referendums approved by the department.<br>2.Write-offs and monitoring. |
| The extent to which CLOs have been achieved | Program leaders - faculty members. | 1.Review the course report.<br>. |
| Other | | |

**Assessor** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
**Assessment Methods** (Direct, Indirect)

## G. Specification Approval Data

| | |
|---|---|
| COUNCIL /COMMITTEE | Department of Applied Sciences – Applied College |
| REFERENCE NO. | |
| DATE | |

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

# Course Specification

هيئة تقويم التعليم والتدريب
Education & Training Evaluation Commission

T-104
2022

# Course Specification

| | |
|---|---|
| Course Title: | NetworkSecurity |
| Course Code: | 0216 شبك |
| Program: | Cybersecurity - Networks |
| Department: | Applied Sciences |
| College: | Applied College |
| Institution: | Imam Mohammad Bin Saud Islamic University |
| Version: | 1st version |
| Last Revision Date: | 2023/02/26 |

# Table of Contents:

# A. General information about the course:

| Course Identification | | | | | |
|---|---|---|---|---|---|
| **1. Credit hours:** | 3 (2 Theory, 2 lab) | | | | |
| **2. Course type:** | | | | | |
| a. | University ☐ | College ☐ | Department☒ | Track☐ | Others☐ |
| b. | Required ☒ | Elective☐ | | | |
| **3. Level/year at which this course is offered:** 3rd Level | | | | | |
| **4. Course general Description:** Students explore how information is exchanged on the Internet and the security issues that arise due to information exchange between different technologies. Students learn concepts of authentication, authorization, access control in network security. Students gain knowledge about Use of cryptography for data and network security. Students are introduced to the topics such as firewalls, public key infrastructure, security standards and protocols, virtual private networks, and wireless network security. | | | | | |
| **5. Pre-requirements for this course (if any):** | | | | | |
| **6. Co- requirements for this course (if any):** N/A | | | | | |
| **7. Course Main Objective(s):** | | | | | |

## 1. Teaching mode (mark all that apply)

| No | Mode of Instruction | Contact Hours | Percentage |
|---|---|---|---|
| 1. | Traditional classroom | | |
| 2. | E-learning | | |
| 3. | Hybrid<br>• Traditional classroom<br>• E-learning | 60 | 100% |
| 4. | Distance learning | | |

## 2. Contact Hours (based on the academic semester)

| No | Activity | Contact Hours |
|---|---|---|
| 1. | Lectures | 12 |
| 2. | Laboratory/Studio | 48 |
| 3. | Field | |
| 4. | Tutorial | |
| 5. | Others (specify) | 150 |
| | Total | 210 |

# B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods

| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 1.0 | Knowledge and understanding | | | |

| Code | Course Learning Outcomes | Code of CLOs aligned with program | Teaching Strategies | Assessment Methods |
|---|---|---|---|---|
| 1.1 | Understand basic concept of how to protect and design private network. | ع1، ع5 | Class lectures.<br>Class discussion.<br>Questions/Answers session in class.<br>Home work.<br>Learning by discovery.<br>Self-education.<br>Brainstorming.<br>Online search.<br>KWL learning table.<br>Mind maps.<br>Concept maps. | Quizzes.<br>Homework and Assignments.<br>Written and online exams.<br>Writing reports.<br>Presentations.<br>Discussion and debate.<br>Achievement file.<br>Performance |
| 1.2 | Understand how to protect security of information | ع1، ع5 | | |
| 1.3 | Use theoretical and practical knowledge in securing data transfer and authentication | ع1، ع5 | | |
| 2.0 | Skills | | | |
| 2.1 | Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats) | ع1، ع5 | Class lectures.<br>Class discussion.<br>Questions/Answers session in class.<br>Home work.<br>Learning by discovery.<br>Self-education.<br>Brainstorming.<br>Online search.<br>Mind maps.<br>Concept maps. | Quizzes.<br>Homework and Assignments.<br>Written and online exams.<br>Writing reports.<br>Presentations.<br>Discussion and debate.<br>Achievement file.<br>Performance tests. |
| 2.2 | Architectures for secure networks (e.g., secure channels, secure routing protocols, secure DNS, VPNs, anonymous communication protocols, isolation) | ع1، ع5 | | |
| 2.3 | Use of cryptography for data and network securit | ع1، ع5 | | |
| 3.0 | Values, autonomy, and responsibility | | | |
| 3.1 | Collaboration, teamwork, and professional ethics. | ق1 | Class lectures.<br>Class discussion.<br>Questions/Answers session in class.<br>Home work.<br>Learning by discovery.<br>Self-education.<br>Brainstorming.<br>Online search.<br>Mind maps.<br>Concept maps. | Quizzes.<br>Homework and Assignments.<br>Written and online exams.<br>Writing reports.<br>Presentations.<br>Discussion and debate.<br>Achievement file.<br>Performance. |
| 3.2 | Take the responsibility for continuous learning, and self-development. | ق2 | | |
| 3.3 | Effective and efficient time management when applying acquired knowledge and skills. | ق3 | | |

## C. Course Content

| No | List of Topics | Contact Hours |
|---|---|---|
| 1. | **Introduction:**<br>○ Computer Security Concepts<br>○ The OSI Security Architecture<br>○ Security Attacks<br>○ Security Services<br>○ Security Mechanisms<br>○ A Model for Network Security | 4 |
| 2. | **Network Security:**<br>○ Security Through Network Devices<br>○ Security Through Network Technology<br>○ Security Through Network Design Elements | 8 |
| 3 | **Firewalls:**<br>○ The Need for Firewalls<br>○ Firewall Characteristics<br>○ Types of Firewalls<br>○ Firewall Basing<br>○ Firewall Location and Configurations | 8 |
| 4 | **Cryptography:**<br>○ Algorithms<br>○ Hashing Functions<br>○ Symmetric Encryption<br>○ Asymmetric Encryption | 3 |
| 5 | **Public Key Infrastructure:**<br>○ The Basics of Public Key Infrastructures<br>○ Certificate Authorities<br>○ Registration Authorities<br>○ Certificate Repositories<br>○ Trust and Certificate Verification<br>○ Digital Certificates | 4 |
| 6 | **Security Standards and Protocols:**<br>○ PKIX and PKCS<br>○ X.509<br>○ SSL/TLS<br>○ ISAKMP<br>○ CMP<br>○ PGP<br>○ HTTPS<br>○ IPsec<br>○ Common Criteria for Information Technology Security (Common Criteria or CC)<br>○ ISO/IEC 27002 | 5 |
| 7 | **Authentication and Remote Access:**<br>○ The Remote Access Process<br>○ SSH/Telnet | 5 |

| | | |
|---|---|---|
| | ○ IEEE 802.1X<br>○ RADIUS<br>○ TACACS+<br>○ Authentication Protocols<br>○ FTP/FTPS/SFTP<br>○ VPNs<br>○ IPsec<br>○ Vulnerabilities of Remote Access Methods | |
| 8 | **IDS/IPS**<br>○ Explain the functions and operations of IDS and IPS systems.<br>○ Describe the characteristics of IPS signatures | 4 |
| 9 | **Virtual Private Networks:**<br>○ VPN Fundamentals<br>○ VPN Management<br>○ VPN Technologies | 4 |
| 10 | **Wireless Network Security:**<br>○ Introduction to Wireless Networking<br>○ 802.11Attacking, New Security Protocols, and Implementation | 3 |
| Total | | 48 |

## D. Students Assessment Activities

| No | Assessment Activities * | Assessment timing (in week no) | Percentage of Total Assessment Score |
|---|---|---|---|
| 1. | Mid-term | Week 7 | 20% |
| 2. | Quizzes (From 3-4 Quizzes) | Week 5, 10 | 10% |
| 3. | 1st Practical Evaluation | Week 2-11 | 15% |
| 4 | project | Week 11 | 20% |
| 5 | Participation | Week 1-11 | 5% |
| 6 | Final | Week 12 | 30% |
| 7 | Total Marks | | 100% |

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

# E. Learning Resources and Facilities

## 1. References and Learning Resources

| | |
|---|---|
| Essential References | ○ Network Security, Firewalls, and VPNS, by J. Michael Stewart, 2010, ISBN 10: 076379130X<br>○ Cryptography and Network Security: Principles and Practices by W.Stallings, Prentice Hall, 5 th Edition, ISBN-10: 0136097049<br>○ Principles of Computer Security: CompTIA Security+ and Beyond by Wm.A. Conklin et al., McGraw Hill, 3 rd Edition, ISBN-10: 0071786198 |
| Supportive References | N/A |
| Electronic Materials | Online resources will be provided during class lectures on LMS. |
| Other Learning Materials | N/A |

## 2. Required Facilities and equipment

| Items | Resources |
|---|---|
| Facilities<br>(Classrooms, laboratories, exhibition rooms, simulation rooms, etc.) | Classroom – A computer lab equipped and connected to a shared printer and the internet. |
| Technology equipment<br>(projector, smart board, software) | Smart board, data projector, Microsoft Visio or Edraw Max and Internet browser. |
| Other equipment<br>(depending on the nature of the specialty) | N\A |

# F. Assessment of Course Quality

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| Effectiveness of teaching | Peer references – students. | 1.Questionnaires and referendums approved by the department.<br>2.Peer evaluation of faculty members.<br>3.Review the results of the students' evaluation. |
| Effectiveness of students assessment | Peer references - program leaders - faculty members – students. | 1.Questionnaires and referendums approved by the department.<br>2.Review course descriptions and course reports periodically. |

| Assessment Areas/Issues | Assessor | Assessment Methods |
|---|---|---|
| | | 3.Peer evaluation and periodic exchange of correction and scrutiny among fellow faculty members.<br>4.Review samples of students' work. |
| Quality of learning resources | Program leaders - faculty members - students | 1.Questionnaires and referendums approved by the department.<br>2.Write-offs and monitoring. |
| The extent to which CLOs have been achieved | Program leaders - faculty members. | 1.Review the course report.<br>2. Analysis of exams forms, grades, students' work and records of achievement. |
| Other | | |

**Assessor** (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)
**Assessment Methods** (Direct, Indirect)

## G. Specification Approval Data

| | |
|---|---|
| COUNCIL /COMMITTEE | Department of Applied Sciences – Applied College |
| REFERENCE NO. | |
| DATE | |