جامعة أم القرى

كلية الحاسب الآلي ونظم المعلومات

الماجستير في الأمن السيبراني

4. Learning and Teaching

4/1 Learning Outcomes and Graduate Specifications

4/1/1 Main tracks or specializations covered by the program:

(a) Cyber Security

(b)

(c)

4/1/2 Curriculum Study Plan Table

Level	Course Code	Course Title	Required or Elective	Prerequisite Courses	Credit Hours
Level 1	140360X-3	Core Course 1	Required	Graduate Standing	3
	140360X-3	Core Course 2	Required	Graduate Standing	3
Level 2	140360X-3	Core Course 3	Required	Graduate Standing	3
	140360X-3	Core Course 4	Required	Graduate Standing	3
Level 3	140360X-3	Core Course 5	Required	Graduate Standing	3
	140361X-3	Core Course 6	Required	Graduate Standing	3
Level 4	140361X-3	Elective Course 1	Elective	Graduate Standing	3
	140361X-3	Elective Course 2	Elective	Graduate Standing	3
Level 5	140361X-3	Elective Course 3	Elective	Graduate Standing	3
	140361X-3	Elective Course 4	Elective	Graduate Standing	3
Level 6	140361X-3	Elective Course 5	Elective	Graduate Standing	3
	140361X-3	Elective Course 6	Elective	Graduate Standing	3
Level 7	140361X-3	Elective Course 7	Elective	Graduate Standing	3
	140369X-3	Research Project	Required	Graduate Standing	3

Course List and Categories

Category	Course Code	Course Title
Core Courses	1403601-3	Principles of Cybersecurity
	1403602-3	Cryptography Engineering
	1403603-3	Network Security
	1403604-3	Software Security
	1403605-3	Cybersecurity Risk Management
	1403606-3	Cybercrimes and Digital Forensics
	1403691-3	Research Project 1
Elective Courses	1403610-3	Secure Communications
	1403611-3	Cloud Computing Security
	1403612-3	Big Data Analytics and Security
	1403613-3	IT Security Management
	1403614-3	Modern Applications of Cybersecurity
	1403615-3	Ethical Hacking
	1403616-3	Security Protocols Engineering
	1403617-3	Special Topics
Research Project Course	1403692-3	Research Project 2

4/1/4. Course Specification:

COURSE SPECIFICATIONS

Form

Course Title: Principles of Cybersecurity

Course Code: 1403601-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Principles of Cybersecurity and 1403601-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

- The importance of taking a multi-disciplinary approach to cyber security
- The cyber threat landscape, both in terms of recent emergent issues and those issues which recur over time
- The roles ad influences of governments, commercial and other organizations, citizens and criminals in cyber security affairs
- General principles and strategies that can be applied to systems to make them more robust to attack
- Key factors in cyber security from different disciplinary views including computer science, management, law, criminology and social sciences
- Issues surrounding privacy, anonymity and pervasive passive monitoring

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This module aims to give a multi-disciplinary overview of cyber security, emphasizing the importance of considering not only technical measures and defenses, but also the other subject areas that apply, including legal, management, crime, risk, social and human factors.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
The cyber security threat landscape, history and evolution	1	3
Security surfaces; intelligence, case studies, trend analysis.	2	3
Actors in cyber security; governments, organisations, citizens, criminals.	3	3
The multidisciplinary nature of cyber security.	4	3
Pervasive passive monitoring.	5	3
ISPs as intermediaries DP	6	3
Principles of secure communications; digital signatures, PKI, encryption, hashing.	7	3

Introduction to biometrics.	8	3
Privacy and anonymity.	8	3
Anonymity protocols; crowds, onion routing, ToR.	9	3
Offensive cyber attacks, cyber war, hacktivism.	9	3
Advanced Persistent Threats.	10	3
Critical infrastructures.	10	3
Case study: the Domain Name Systems.	11	3
Case study: eCash, Bitcoin.	11	3
Security aspects of social networks, the web science perspective - Management of cyber risks.	12	3
Multilevel security, security policies.	12	3
Security economics; investment, cost of breach.	13	3
Data management.	13	3
anonymisation and de-anonymisation.	13	3
Cyber law, regulating the online environment.	14	3
Computer access offences, data protection law	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		

1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- Hadnagy, C (2011). Social Engineering: The Art of Human Hacking.
- Andress, J. (2013). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.
- Clarke, R.A. (2012). Cyber War: The Next Threat to National Security and What to Do about it.
- Graham, J., Howard, R. and Olson, R. (2011). Cyber Security Essentials.

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Cryptography Engineering

Course Code: 1403602-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Cryptography Engineering and 1403602-3
2. Credit hours: 3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

Cryptography Engineering provides the gateways through which electronic commerce will flow in the future Internet. Most technologies that shape tomorrow's society will be built around these gateways which will enable real-time purchase, distribution, and delivery of multimedia content to the homes, while securing the intellectual property rights and the royalty streams of authors, artists, producers, and publishers. These gateways will allow mass customization of information to individual and corporate consumers by letting people turn their driver's licenses into digital wallets that carry anything from electronic cash to credit lines, airline tickets, or medical prescriptions. The creation of distributed universities, virtual communities, and millions of micro businesses around the world are not too far in the future.

Cryptography provides the information security technology necessary tools and methods for the construction of this infrastructure in such a way that the privacy, ownership rights, and consumer rights of the participants are protected. We will study theoretical aspects of cryptographic algorithms and security protocols, and show how these techniques can be applied to solve particular data storage, networking, communication security, rights management problems. In this course, we are particularly interested in security for ubiquitous computing, embedded systems and devices, and peer-to-peer computing.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction and Classical Cryptosystems	1	3
Steganography	2	3
Overview of Cryptography	3	3
Classic Cryptosystems	4, 5	6

RSA & Number Theory	6, 7	6
RSA Hardware Architectures	9	3
Elliptic Curve Cryptography (ECC)	10	3
ECC Hardware Issues	11, 12	6
Symmetric Key Cryptosystems	13	3
Crypto Remarks	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports

4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester			
	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	**Week Due**	**Proportion of Total Assessment**
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Orschot and Scott A. Vanstone
- Modern Cryptography Protect Your Data with Fast Block Ciphers, Nik Goots, Boris Izotov, Alex Moldovyan, Nik Moldovyan
- Cryptography Theory and Practice, Doug Stinson
- W. Trappe & L. C. Washington. Introduction to Cryptography with Coding Theory

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Network Security

Course Code: 1403603-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Network Security and 1403603-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

The course covers state-of-art computer networks security topics. Students will be able to evaluate the risks faced by computer and network systems, detect common vulnerabilities, use proper methods to protect their systems and networks, and more importantly, apply the learned security principles to solve real-world problems. Topics include Packet sniffing. Firewall, DNS attack and many others. For each network security topic, the course uses a series of hands-on activities to help explain the principle; so that the students can "touch", play with, and experiment with the principle, instead of just reading about it.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Packet Sniffing and Spoofing	1, 2	6
Attacks on the TCP protocol	3, 4	6
Firewall	5	3
DNS and attacks	7, 8	6
VPN Security	10, 11	6
The Heartbeat Bug and attack	12, 13	6
PKI Infrastructure	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week.	3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week): Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks Computer Security: A Hands-on Approach 1st Edition by Wenliang Du
2. List Essential References Materials (Journals, Reports, etc.) - IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator

- Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Software Security

Course Code: 1403604-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Software Security and 1403604-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

- **Define system software components and their security issues**
- **Evaluate the security of system software components**
- **Design a secure system software**
- **Identify software flaws and vulnerabilities**

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This course focuses on the security aspects of diffident system software components, including operating systems (OS), compilers, interpreters, and software utilities. It will study OS level mechanisms and policies in investigating and defending against real-world attacks on computer systems. In addition, the course will introduce and survey the emerging field of "Language-based Security", in which techniques from compilers and programming language theory are leveraged to address issues in computer security. Furthermore, the course will cover security utility design principles, and the vulnerabilities caused by software flaws. .

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction	1	3
Operating systems security	2, 3, 4, 5	12
Information flow	6, 7	6
Compiler-based security	8	3
Language-based security	10, 11	3
Security utilities	12	3
Software flaws and vulnerabilities	13, 14	6
Case studies and examples	15	6

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%

2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

There is no approved textbook for this course. Readings will be based on extracts from books, copies of published papers, and online resources.

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching

- Online form available throughout the semester, which is automatically directed to the program coordinator
- Hardcopy student survey forms are collected at the end of the semester

2. Other Strategies for Evaluation of Teaching by the Instructor or the Department

- Instructor: getting student feedback orally through lectures and office hours
- Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.

3. Procedures for Teaching Development

- Circulating student feedback to instructors
- Awards for teaching excellence
- Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution)

Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.

5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it.

The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Cyber Security Risk management

Course Code: 1403605-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Cyber Security Risk management and 1403605-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

- **Identify different types of risks, threats and vulnerabilities.**
- **Understand how to develop a compliance assessment plan and employ a standards-based risk management process while maintaining a satisfactory security posture.**
- **Implement standards-based, proven methodologies for assessing and managing the risks to organization's information infrastructure**
- **Select security controls that ensure compliance with applicable laws, regulations, policies, and directives**

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This course focuses on how to conduct a security risk assessment to protect organizations. It covers laws and regulations that impose strict cyber security requirements on all organizations. The course builds knowledge on analyzing new threats and vulnerabilities, performing security assessments, and providing a technology audit function.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction to Risk Management	1	3
Risk Management lifecycle	2, 3	6
Risk assessment and analysis	4, 5	6
Risk mitigation strategies	7, 8	6
Risk assessment techniques	10, 11	6
Risk management programs	12, 13	6
Case studies and examples	14, 15	6

2. Course components (total contact and credit hours per semester):

	Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total

Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%

3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

Evan Wheeler,"Security Risk Management: Building an Information Security Risk Management Program from the Ground Up", Elsevier, 2011

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching

- Online form available throughout the semester, which is automatically directed to the program coordinator
- Hardcopy student survey forms are collected at the end of the semester

2. Other Strategies for Evaluation of Teaching by the Instructor or the Department

- Instructor: getting student feedback orally through lectures and office hours
- Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.

3. Procedures for Teaching Development

- Circulating student feedback to instructors
- Awards for teaching excellence
- Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution)

Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.

5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it.

The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Cybercrimes and Digital Forensics

Course Code: 1403606-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Cybercrimes and Digital Forensics and 1403606-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

This course provides an introduction to the methodology and procedures associated with digital forensic analysis in a network environment. Students will develop an understanding of the fundamentals associated with the topologies, protocols, and applications required to conduct forensic analysis in a network environment. Students will learn about the importance of network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. This course will incorporate demonstrations and laboratory exercises to reinforce practical applications of course instruction and will require an independent research paper related to the course topic.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction to Network Forensics and Investigating Logs	1, 2	6
Network Traffic Investigations	3, 4	6
Web Attack Investigations	5	3
Router Forensics	7, 8	6
Denial of Service Investigations	9	3
Internet Crime Investigations	10	3
Email Crime Investigations	12	3
Wireless Attack Investigations	13	3
PDA Forensics	14	3
iPod and iPhone Forensics		

Blackberry Forensics		
Corporate Espionage Investigations		
Trademark and Copyright Investigations		

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		

4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester			
	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	**Week Due**	**Proportion of Total Assessment**
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

A. Computer Forensics : Investigating Network Intrusions and Cyber Crime, EC-Council, ISBN-13: 978-1-4354-8352-1, ISBN-10: 1-4354-8352-9

B. Computer Forensics : Investigating Wireless Networks and Devices, EC-Council, ISBN-13: 978-1-4354-8353-8, ISBN-10: 1-4354-8353-7

C. Handbook of Digital Forensics and Investigations, Eoghan Casey ed., Elsevier Academic Press, ISBN 13: 978-0-12-374267-4-

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed: _____**

Program Coordinator: _____

Signature: _____ **Date Received: _____**

COURSE SPECIFICATIONS

Form

Course Title: Secure Communications

Course Code: 1403610-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Secure Communications and 1403610-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

Secure Communications as a discipline, addresses the prevention of unauthorized access to telecommunications traffic or any information that is either transferred or transmitted in by electrical means. Communications Security serves as a protective shield for electronic emissions associated with sensitive information: a process involving the usage of specialized technical, operational and physical security measures. Hence, effective and secure communication can deliberately lead to creating trust for both internal and external parties within the organizational reach. Communications Security raises awareness and understanding for cautiousness whilst handling sensitive information. By following the steps indicated by updated standard secure structured framework strategy, communications can maintain protecting sensitive and classified information reducing threats possibility. The course briefs network security mechanisms and protocols, network access authentication, wireless security, and radio air link protection. It details broadcast and multicast key distribution, trust platforms, temple response hardware, and physical layer security. Some special topics on attacks, privacy model, and RFID for counterfeiting will be covered.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Security Architecture Evolution of Communication Systems	1, 2	6
Historical Developments of Secure Communications and Cryptographic Primitives	3, 4	6
Basics of Protected Communication	5	3
Basic Information Security Concepts and Protection Mechanisms	7, 8	6
Trust Model and Threat Model Security Components	10, 11	6
Security in 4G-LTE Cellular System	12	3
Protection of Wireless Link UMTS/4G-LTE AKA and Air Link Protection	13	3
Some forgery Attacks on 4G-LTE Authentication Protection	14	3

2. Course components (total contact and credit hours per semester):							
		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week.	3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester			
	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment

1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- L.D. Chen and G. Gong, Communication System Security, CRC, 2012.
- Man Young Rhee, Mobile Communication Systems and Security, 2009, Wiley-IEEE Press
- Some notes and supplement materials prepared by the instructor.

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Cloud Computing Security

Course Code: 1403611-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Cloud Computing Security and 1403611-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

This course focuses on these security concerns and countermeasures for a cloud environment. An overview of cloud computing and virtualization, the critical technology underpinning cloud computing, provides the necessary background for these threats. Additional topics vary but may include access control, identity management, denial of service, account and service hijacking, secure APIs, malware, forensics, regulatory compliance, trustworthy computing, and secure computing in the cloud. This course follows a seminar-style format where students are expected to lead class discussions and write a publication-quality paper as part of a course project.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Virtualization	1, 2	6
Trusthworthy computing	3, 4	6
Secure Computation	5	3
Cloud Management	7, 8	6
Data Management	10, 11	6
Data Security	12	3
Regulatory Compliance	13	3
Forensics and Malware	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact	Planned	45	---	---	---	---	45

Hours	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%

3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler (Syngress/Elsevier) - 978-1-59749-592-9 o Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563
-

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching

- Online form available throughout the semester, which is automatically directed to the program coordinator
- Hardcopy student survey forms are collected at the end of the semester

2. Other Strategies for Evaluation of Teaching by the Instructor or the Department

- Instructor: getting student feedback orally through lectures and office hours
- Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.

3. Procedures for Teaching Development

- Circulating student feedback to instructors
- Awards for teaching excellence
- Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution)

Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.

5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it.

The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Big Data Analytics and Security

Course Code: 1403612-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Big Data Analytics and Security and 1403612-3
2. Credit hours: 3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)	☐	percentage?	☐
c. E-learning	☐	percentage?	☐
d. Correspondence	☐	percentage?	☐
f. Other	☐	percentage?	☐

Comments:

B Objectives

1. The main objective of this course

- employ the Data Analytics Lifecycle to address Big Data analytics projects.
- explain how to structure data analysis and get values out of Big Data.
- describe the landscape of Big Data Analytics by exploring several examples of real world problems.
- explain the impact of Big Data on data collection, data analysis, data reporting, data monitoring, and data storage.
- apply appropriate Splunk's analytic techniques and tools to analyze Big Data.
- identify the possible problems that are associated with Big Data.
- reorganize the possible problems that are associated with Big Data as data science questions.
- install and run programs by using tools such as R and RStudio, MapReduce/Hadoop.
- build alerts and create simple reports and dashboards with Splunk.
- identify the threats affecting Big Data.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This course provides a fundamental and introductory-level overview of the field of Big Data and related security topics to enable effective participation in Big Data and other analytics projects as a practitioner. It provides students with an opportunity to search, navigate, tag, build alerts, and create simple reports and dashboards with Splunk. The course begins with an introduction to Big Data and the data analytics lifecycle to address business challenges that leverage Big Data. It also provides grounding in basic analytic methods and an introduction to Big Data analytics technology and tools, including MapReduce, Splunk, and Hadoop. This course employs both "open source technology" (Hadoop) and "commercial technology" (Splunk). This course is for those new to the Big Data field as well as the security threat landscape. No prior programming experience or statistics background is required. An EMCDSA (Big Data industry) certification exam is part of this course.

1. Topics to be Covered		
List of Topics	**No. of Weeks**	**Contact hours**
Introduction to Big Data Analytics	1	3
Data Analytics Lifecycle	2	3
Analytics - Theory And Methods	3	3
Analytics - Technologies and Tools	4	3
Big Data Threat	5	3
Gap Analysis	6	3
The Endgame, or Putting it All Together	8	3
Saving Results and Searches	9	3
Using Fields	10	3
Tags and Event Types	12	3
Creating Alerts	13	3
Creating Reports	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		

1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- Practical Internet of Things Security (Kindle Edition) by Brian Russell, Drew Van Duren
- Securing the Internet of Things Elsevier
- Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations.

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: IT Security Management

Course Code: 1403613-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: IT Security Management and 1403613-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 1 or 2.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

a) Analyse and discuss the significance of IT security management for organisations;
b) Develop and implement IT security management structure for small, medium and large size businesses and corporations;
c) Evaluate on the security of the existing organisation architecture, data, application, technology, etc;
d) Investigate and discuss for the appropriate design and secure solution for varieties of organisations;
e) Implement a process to support the administration and the management of organisations' security;
f) Conduct practical investigations into Network Systems including industry procedures of Information Gathering, Vulnerability Identification, Exploitation and privilege escalation.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This is a third trimester core unit out of a total of 12 units in the Master of Networking (MNet). This unit addresses the MNet course learning outcomes and complement other courses in a related field by developing students' specialized knowledge in network advance security and applying critical skills in networking security such as hacking skills, computer hardening and vulnerabilities. For further course information refer to: http://www.mit.edu.au/courses/master-networking. This unit is part of the AQF level 9 (MNet) course.

This unit provides students with understanding and appreciation of the discipline of IT Information Security Management. They will also learn how information security management

interacts with other organisational groups, especially with general management and with information technology groups.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction to the management of information security	1, 2	6
Planning for information security	3, 4	6
Planning for contingencies	5	3
Information Security Policy	7, 8	6
Developing the security program	10	3
Security Management Practices	11	3
Risk Management: identifying and assessing risk	12	3
Risk Management: Assessing and controlling risk	13	3
Protection Mechanisms	14	3

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- Michael E. Whitman and Herbert J. Mattord, *"Management of Information Security"*, 4th Edition: 9781285062297
- Michael E. Whitman, "*Hands-on Information Security*" Lab Manual 4th Edition. 9781285167572

• Alfred Basta, Nadine Basta and Mary Brown, *"Computer Security and Penetration"* Testing 2nd edition 9780840020932
2. List Essential References Materials (Journals, Reports, etc.) - IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access,etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence

- Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed: _____**

Program Coordinator: _____

Signature: _____ **Date Received: _____**

COURSE SPECIFICATIONS

Form

Course Title: Modern Applications of Cybersecurity

Course Code: 1403614-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Modern Applications of Cybersecurity and 1403614-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 2 or 3.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

- **Have a wide knowledge of cybersecurity applications**
- **Be familiar with different security techniques used in different sectors**
- **Design a secure system for a specific application**

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This course covers the application of cybersecurity in different fields of life. Modern techniques of security applied in different sectors should be reviewed and discussed.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction (1 week)	1	3
Cybersecurity for e-commerce (2 weeks)	2, 3	6
Cybersecurity for banking (2 weeks)	4, 5	6
Cybersecurity for healthcare (2 weeks)	7, 8	6
Cybersecurity for government (2 week)	10, 11	6
Cybersecurity for tourism(2 weeks)	12, 13	6
Cybersecurity for industry and plant control(2 weeks)	14, 15	6

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week.	3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week): Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks There is no approved textbook for this course. Readings will be based on extracts from books, copies of published papers, and online resources.
2. List Essential References Materials (Journals, Reports, etc.) - IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator

- Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Ethical Hacking

Course Code: 1403615-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Ethical Hacking and 1403615-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 2 or 3.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

Study fundamental principles and techniques of ethical hacking. Students would learn how hackers attack computers and networks, and how to protect them against these attacks. Students would also get hand-on experience through multiple assignments and mini projects.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

- Introduction to ethical hacking and code of ethics
- Penetration testing life cycle
- Footprinting and Social Engineering
- Port Scanning
- Microsoft Operating System Vulnerabilities
- Linux Operating System Vulnerabilities
- Hacking Web Servers
- Hacking Wireless Networks
- Hacking Mobile Applications

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Course Outlines, Introduction to ethical hacking and code of ethics	1	3
Penetration testing life cycle	2	6
Footprinting and Social Engineering	2	6
Port Scanning	1	3
Microsoft Operating System Vulnerabilities	2	6
Review and Exam	1	3
Linux Operating System Vulnerabilities	2	6
Hacking Web Servers	1	3
Hacking Wireless Networks	1	3
Hacking Mobile Applications	2	6

2. Course components (total contact and credit hours per semester):							
		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week.	3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester			
	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment

1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

- The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, by Patrick Engebretson
- Hands-On Ethical Hacking and Network Defense, by Michael T. Simpson

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Security Protocols Engineering

Course Code: 1403616-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Security Protocols Engineering and 1403616-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 2 or 3.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

- **Appreciate security protocol design methodology**
- **Evaluate the security of different protocols and systems**
- **Assess and monitor overall security of a system**
- **Design and use security testing tools**

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

The course focuses on the design, implementation, and maintenance aspects of security protocols and mechanisms. Students will learn to analyze protocols and systems in terms of their security properties. They will also learn about the challenges faced in the implementation of such systems, along with possible solutions. Security issues in cryptographic protocols, operating systems, networks as well as applications will be considered. Students will gain hands-on experience in the design of security protocols and the use of appropriate tools for the analysis of secure systems.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
Introduction (1 week)	1	3
Applications security (2 weeks)	2, 3	6
Operating systems security (2 weeks)	4, 5	6
Network security (2 weeks)	6	3
Distributed systems security (1 weeks)	7	3
Issues in analysis of security protocols (1 week)	9	3
Monitoring and administration (2 weeks)	10, 11	6
Case studies from current systems (2 weeks)	12, 13	6

2. Course components (total contact and credit hours per semester):

	Lecture	Tutorial	Laboratory/	Practical	Other	Total

				Studio			
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%

3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks

There is no approved textbook for this course. Readings will be based on extracts from books, copies of published papers, and online resources.

2. List Essential References Materials (Journals, Reports, etc.)

- IEEE related journals and conference papers
- ACM related journals and conference papers
- Springer related journals and conference papers
- Elsevier related journals and conference papers

3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.

4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)

1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.

2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.

3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development - Circulating student feedback to instructors - Awards for teaching excellence - Circulating courses between different instructors
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____

COURSE SPECIFICATIONS

Form

Course Title: Special Topics

Course Code: 1403617-3

Date: 09/12/2018	**Institution**: Umm Al-Qura University
College: Computers and Information Systems	**Department**: Computer Engineering

A. Course Identification and General Information

1. Course title and code: Special Topics and 1403617-3
2. Credit hours:3.
3. Program(s) in which the course is offered: Master of Cyber Security.
4. Name of faculty member responsible for the course: Faculty members within the college of Computers and Information Systems, specialized in the area.
5. Level/year at which this course is offered: Year 2 or 3.
6. Pre-requisites for this course (if any): Graduate Standing.
7. Co-requisites for this course (if any): N/A.
8. Location if not on main campus: Male/Female Campus.
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	■	percentage?	100%
b. Blended (traditional and online)		percentage?	
c. E-learning		percentage?	
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course

Discuss new topics which are selected from current literature in the field of Cyber Security. One or more areas within the field will be explored in details.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field):

- University digital library has subscriptions in many research databases with state-of-the-art materials in the area.

- The whole program with all its courses is reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This course is intended to teach modern theory and practices in the field of Cyber Security. The course would have assignments and project for students to get hands on experience. Students should provide their findings through oral presentation and in writing.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
To be decided by the course instructor (TBD)	1-15	45

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	---	---	---	---	45
	Actual						
Credit	Planned	3	---	---	---	---	3
	Actual						

3. Individual study/learning hours expected for students per week. 3

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Have thorough knowledge and critical understanding of the main areas of the field of Cyber Security	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
2.0	**Cognitive Skills**		
2.1	Make informed and defensible judgments in circumstances where there is an absence of complete or consistent information	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
3.0	**Interpersonal Skills & Responsibility**		
3.1	Take initiative in identifying and responding creatively to complex issues and problems in an academic or professional context	Lectures and Group discussion	Exams, Quizzes, Homework, and Reports
4.0	**Communication, Information Technology, Numerical**		
4.1	Use a wide range of appropriate information and communications technology in investigating issues	Lectures, Group discussion, Projects, and Seminars	Exams, Reports, and Presentations

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Final Exam	16-17	50%
2	Midterm Exam	8-10	20%
3	Other Semester Work (Quizzes, Assignments, Projects, Essay, Presentation … etc)	Throughout the semester	30%

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week):
Course Instructor would dedicate at least two office hours in two different days of the week.

E. Learning Resources

1. List Required Textbooks To be decided by the course instructor.
2. List Essential References Materials (Journals, Reports, etc.) - IEEE related journals and conference papers - ACM related journals and conference papers - Springer related journals and conference papers - Elsevier related journals and conference papers
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc.
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.): Ordinary classroom.
2. Technology resources (AV, data show, Smart Board, software, etc.): Data-show, PC/Laptop with a presentation software installed, ordinary while board.
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G. Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - Online form available throughout the semester, which is automatically directed to the program coordinator - Hardcopy student survey forms are collected at the end of the semester
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - Instructor: getting student feedback orally through lectures and office hours - Program Administrators: Follow-up by chair of the department and vice dean of research and scientific research.
3. Procedures for Teaching Development

- Circulating student feedback to instructors
- Awards for teaching excellence
- Circulating courses between different instructors

4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution)

Arbitrary exam papers as well as student samples are checked by independent faculty members within the college.

5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it.

The whole program with all its courses are reviewed and updated every 3-4 years according to the evolution of the discipline in both academia and industry.

Name of Course Instructor: _____

Signature: _____ **Date Completed: _____**

Program Coordinator: _____

Signature: _____ **Date Received: _____**

COURSE SPECIFICATIONS

Form

Course Title: Criminal Psychology

Course Code: .....

Date: 20....–.....–.....	**Institution**: Umm AlQura University.
College: Faculty of Education	**Department**: Department of Psychology

A. Course Identification and General Information

1. Course title and code: Criminal Psychology
2. Credit hours: 3 hourss
3. Program(s) in which the course is offered: An elective course for Master in cyber security

   (If general elective available in many programs indicate this rather than list programs)
4. Name of faculty member responsible for the course: Faculty of Education
5. Level/year at which this course is offered: Third
6. Pre-requisites for this course (if any): -
7. Co-requisites for this course (if any): -
8. Location if not on main campus: Umm AlQura University
9. Mode of Instruction (mark all that apply):

a. Traditional classroom	80	percentage?	80%
b. Blended (traditional and online)	10	percentage?	10%
c. E-learning	10	percentage?	10%
d. Correspondence		percentage?	
f. Other		percentage?	

Comments:

B Objectives

1. The main objective of this course:

This Course is examined the history of crime and punishment and the psychology of the criminal, including criminal behavior and the law, punishment and rehabilitation.

The subjects detailed in the course range from the different theories of why people commit crimes to a detailed examination of the types of crime committed (e.g. murder, sex offences). The course also looks at profiling techniques and other investigative tools (interviewing, lie detection). The course also covers other related topics within legal psychology which has connections with both Forensic Psychology and Criminal Psychology.

2. Describe briefly any plans for developing and improving the course that are being implemented. (e.g. increased use of the IT or online reference material, changes in content as a result of new research in the field)

1. Searching online to find all sites that may help develop the course.

2 - Use the internal network to search for new ideas and developments in this field.

C. Course Description (Note: General description in the form used in the program's bulletin or handbook)

Course Description:

This Course is examined the history of crime and punishment and the psychology of the criminal, including criminal behavior and the law, punishment and rehabilitation.

1. Topics to be Covered

List of Topics	No. of Weeks	Contact hours
1. Criminal psychology: Concept, definition, history, objectives, roles, responsibilities, and skills of criminal psychologist, Relationship between Criminal Psychology and Other Sciences	2	6
2. Normality and Abnormality: definitions, indicators and norms	1	3
3. Personality and Behavior:	1	3
4. Personality: definition, Personal components, Differentiating Normal and Abnormal Personality, Dimensions, and traits.	1	3
5. Motivations: Concept and Maslow theory and criminal behavior.	1	3
6. theoretical models of criminal behavior -Biological, sociological, and psychological theories - Mental disorders and criminal behavior -Islamic perspective	2	6

7. Research methods in criminal psychology - Descriptive research - Experimental research - Historical research	1	3
8. Classification of criminals and crimes	1	3
9. Criminal psychology Technique - free association - hypnosis - Truth Serum -Psychological Test -Personal interview	2	6
10. elements of criminal act - Offender, Witness, Judge, and Investigator	1	3
11. Strategies and rehabilitation in Criminal psychology - insights - behavioural modification -Cognitive-behavioral therapy -Islamic therapy -counseling treatment	2	6

2. Course components (total contact and credit hours per semester):

		Lecture	Tutorial	Laboratory/ Studio	Practical	Other	Total
Contact Hours	Planned	45	-	-	-	-	45
	Actual						
Credit	Planned						
	Actual	3	-	-	-	-	3

3. Individual study/learning hours expected for students per week. 4 hours

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategies

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and targeted learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy should fit in together with the rest to form an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Curriculum Map

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods

1.0	**Knowledge**		
1.1	Determines the importance of criminal psychology in light of the continuance developments	Dialogue and discussion	Writing an article
1.2	Explains the need to develop the capacity of members of society to communicate securely in the light of technological developments	presentation	Assignments
2.0	**Cognitive Skills**		
2.1	suggestion skills that should be provided to community members to encounter the criminal act	presentation	Assignments
2.2	Using new technology in psychological measurement and research	presentation	Assignments
3.0	**Interpersonal Skills & Responsibility**		
3.1	Determines its responsibilities towards the members of society in light of technological changes	Dialogue and discussion	Practical applications
3.2	Shows sensitivity to gaps and scientific problems in scientific research	Dialogue and discussion	Practical applications
4.0	**Communication, Information Technology, Numerical**		
4.1	describe the skills of secure communication through social media and technical means of communication	presentation	Assignments
4.2	using the new technology to explore the mental disorders in the context of successive changes	Practical applications	Practical applications
5.0	**Psychomotor(if any)**		
5.1			
5.2			

5. Assessment Task Schedule for Students During the Semester

	Assessment task (i.e., essay, test, quizzes, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Homework	3,4,9	15%
2	Exam	8	30%
3	Presentation	10	15%
4	Final exam	15	40%
5			
6			
7			
8			

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic counseling. (include the time teaching staff are expected to be available per week)

E Learning Resources

1. List Required Textbooks Francis Pakes, Suzanne Pakes - Criminal Psychology published by Routledge 6 Dec 2012, 184 pages, ISBN 1135846073, Routledge Studies in Development and Society [Retrieved 2015-09-20[Lombroso, Cesare. (1911). Crime, its causes and remedies. Translated by Henry P. Horton. London: Little, Brown. Poythress, N.G. and Hall, J.R. (2011), "Psychopathy and impulsivity reconsidered", Aggression and Violent Behavior, Vol. 16 No. 2, pp. 120-34 . Rogstad, J.E. and Rogers, R. (2008), "Gender differences in contributions of emotion to psychopathy and antisocial personality disorder", Clinical Psychology Review, Vol. 28 No. 8, pp. 1472-84. Stephenson, G. M. (1992). The psychology of criminal justice. Malden, : Blackwell Publishing. Turvey, Brent E. (2002). Criminal Profiling, 4th Edition An Introduction to Behavioral Evidence Analysis. California: Elseiver Science Ltd. ISBN 978-0127050416. Woodworth, M., Freimuth, T., Hutton, E.L., Carpenter, T., Agar, A.D. and Logan, M. (2013), "High-risk sexual offenders: an examination of sexual fantasy, sexual paraphilia, psychopathy, and offence characteristics", International Journal of Law and Psychiatry, Vol. 35 No. 2, pp. 144-56.
2. List Essential References Materials (Journals, Reports, etc.) Simourd, D.J. and Hoge, R.D. (2000), "*Criminal psychopathy a risk-and-need perspective*", *Criminal Justice and Behavior*, Vol. 27 No. 2, pp. 256-72.
3. List Electronic Materials, Web Sites, Facebook, Twitter, etc. https://www.journals.elsevier.com/contemporary-educational-psychology https://en.wikipedia.org/wiki/Contemporary_Educational_Psychology
4. Other learning material such as computer-based programs/CD, professional standards or regulations and software.

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access, etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) -Classrooms equipped with modern presentation data show.
2. Technology resources (AV, data show, Smart Board, software, etc.)

Increasing number of Computers at the Library of the University
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list) **Non**

G Course Evaluation and Improvement Procedures

1. Strategies for Obtaining Student's Feedback on Effectiveness of Teaching - The results of the tests. --Open Discussion with students to present their points of view about the curriculum
2. Other Strategies for Evaluation of Teaching by the Instructor or the Department - A coordinator's survey of students' views on the benefit they have taken from the course study. - Application form on the assessment of the course by the Department of Measurement and Guidance at the University -At the end of the semester, the department analyzes students' results in tests.
3. Procedures for Teaching Development -Periodic review of the issues and topics in the curricula. - Monitoring contemporary societal changes to determine the issues and topics that can be addressed by the curricula - Attend training courses to develop teaching skills
4. Procedures for Verifying Standards of Student's Achievement (e.g. check marking by an independent member teaching staff of a sample of student's work, periodic exchange and remarking of tests or a sample of assignments with staff members at another institution) independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution) - Agreement between those in charge of teaching the course to conduct standardized tests. - Exchange re-correcting tests or a sample of assignments.
5. Describe the planning arrangements for periodically reviewing course effectiveness and planning for developing it. - Regular annual evaluation of the course to identify its strengths and weaknesses and perform necessary improvements. - Regular updating of the course material. - Evaluation of course learning outcome.

Name of Course Instructor: _____

Signature: _____ **Date Completed:** _____

Program Coordinator: _____

Signature: _____ **Date Received:** _____