كلية الهندسة والحاسبات والمعلوماتية

HEKMA SCHOOL OF ENGINEERING, COMPUTING & INFORMATICS

Dar Al-Hekma University

Hekma School of Engineering, Computing & Informatics

HECI

Bachelor of Cybersecurity Program

Bachelor Handbook

Table of Contents

Bachelor of Science in Cybersecurity (BSCY):

The Bachelor of Science in Cybersecurity (BSCY) is a four-year program with 136 credit hours towards graduation. It prepares students to deal with computer viruses, malware and scams, and to protect personal privacy and organizational data from hackers and cyber criminals by setting policies and controls of ethics and risk management. Students learn how to create, operate, analyses, and penetrate computer systems and networks to ensure their security

The BSCY curriculum has been designed with an input from cybersecurity experts to meet the recent ABET Accreditation Criteria and ACM/IEEE guidelines for cybersecurity programs. It includes multiple industry-recognized certifications that are built into the curriculum to support the students' résumés.

BSCY Tracks:

Track 1

Computer Forensics Track

Track 2

Ethical Hacking Track

Track 3

Computer Forensics and Ethical Hacking Track

*Designed according to IEEE CS2013 & ABET (18-19 V2)

Program Mission:

Graduating professionals equipped with design thinking, leadership, and research skills in the fields of Cybersecurity to foster creativity and sustainability.

Program Goals:

- Qualify specialized and distinctive graduates in Cybersecurity to fulfill the requirements of the country.
- Ensure best teaching strategies, alternative methods, and program offerings to meet current and future market needs and students learning differences.
- Communicate effectively in a variety of professional contexts..
- Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
- Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

BCyb Learning Outcomes
Knowledge and Understanding
K1 Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
Skills
S1 Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
S2 Communicate effectively in a variety of professional contexts.
S3 Apply security principles and practices to maintain operations in the presence of risks and threats.
Values
V1 Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.
V2 Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.

Graduate Attributes

- Critical thinking and problem solving
- Design ability
- Communication skills
- Professionalism and ethical competency
- Leadership and teamwork
- Long-life learning
- Deep Cybersecurity knowledge and intellectual breath
- Research capability

Career Prospects:

The program equips students with the necessary knowledge, expertise, and tools to be ready for career opportunities, such as:

1. Information Security Officers
2. Cybersecurity Specialists
3. Cybersecurity Analysts
4. Ethical Hacking Specialists
5. Computer Forensics Specialists
6. Project Managers
7. Information Technology Specialists

Plan of Study:

Year	Semester	Code	Name	Credits	Total in semester
YEAR ONE (1)	Fall	ICTC 1302	Information and Computing Technology Concepts	3	17
		LOGC 1202	Digital Logic Concepts	2	
		ARTS XXXX	Arts and Design	2	
		COMM 1301	Communication Skills I	3	
		ARAB XXXX	Arabic Studies	3	
		MATH 1304	Calculus I	3	
		BSCS 1160	Computer Ethics and Society	1	
	Spring	COMM 1302	Communication Skills II	3	18
		ISLS XXXX	Islamic Studies	3	
		BSCS 1330	Discrete Structures	3	
		BSCS 1350	Introduction to Programming	3	
		BSCS 1320	Computer Architecture and Organization	3	
		BSCY 1310	Fundamentals of Cybersecurity	3	
YEAR TWO (2)	Fall	ISLS XXXX	Islamic Studies	3	18
		STAT 2301	Statistics	3	
		BSCS 2355	Object Oriented Programming	3	
		BSCS 2351	Fundamental Data Structures	3	
		BSCS 2370	Operating Systems	3	
		BSCY 2311	Basic Cryptography Concepts	3	
	Spring	ARAB XXXX	Arabic Studies	3	18
		XXXX XXXX	Required Gen. Ed Electives (HUMN, NASC, SBSC)	3	
		BSCS 2375	Networking and Data Communication	3	
		BSCS 2310	Analysis of Algorithms	3	
		BSIS 2340	IS Project Management	3	
		BSCY 2320	Secure Software Development	3	
YEAR THREE (3)	Fall	EMOI 1201	Emotional Intelligence	2	17
		XXXX XXXX	Free Electives	3	
		BSCS 3345	Human Computer Interaction	3	
		BSCS 3365	Software Engineering	3	
		BSCY 3330	System Components Security	3	
		BSCY 3340	Networks and Connections Security	3	
	Spring	ISLS XXXX	Islamic Studies	2	17
		XXXX XXXX	Free Elective	3	
		BSIS 3320	Database Management Systems	3	
		BSCY 3350	Managing Systems Security	3	
		BSCY 3360	Human Privacy and Security	3	
		BSCY XXXX	Program Elective	3	
YEAR FOUR (4)	Fall	ENTR 3301	Entrepreneurship and Design Thinking	3	18
		XXXX XXXX	Required Gen. Ed Electives (HUMN, NASC, SBSC)	3	
		BSCY 4312	Information Storage Security	3	
		BSCY 4370	Organizational Risk Management and Governance	3	
		BSCY 4391	Capstone Project I	3	
		BSCY XXXX	Program Elective	3	
	Spring	BBBF 1101	Basic Body and Brain Fitness	1	13
		BSCY 4380	Societal Security and Cyber Law	3	
		BSCY 4392	Capstone Project II	3	
		BSCY 4393	Internship	3	
		BSCY XXXX	Program Elective	3	

General Electives		**CH**
BSCY 3301	IT Audit and Controls	3
BSCY 3302	Emerging Technologies in Cybersecurity	3
BSCY 3390	Research Methods in Cybersecurity	3
Electives: Ethical Hacking Track		**CH**
BSCY 3304	Ethical Hacking Concepts	3
BSCY 4305	Web Applications Ethical Hacking	3
BSCY 4306	Network Ethical Hacking	3
Electives: Computer Forensics Track		**CH**
BSCY 3307	Computer Forensics Investigations	3
BSCY 4308	Network Forensics and Analysis	3
BSCY 4309	Mobile Forensics and Analysis	3

University Requirement		19
Ministry Requirement		14
Required General Elective		6
Free Elective		6
ABET (18/19V2)	Program Requirement (Math, Stat)	9
	Computing Department Requirement	34
	Program Requirement (CY Core Knowledge)	39
	Program Elective	9
Total credit hours for graduation		**136**

Double Track (Ethical Hacking and Computer Forensics)

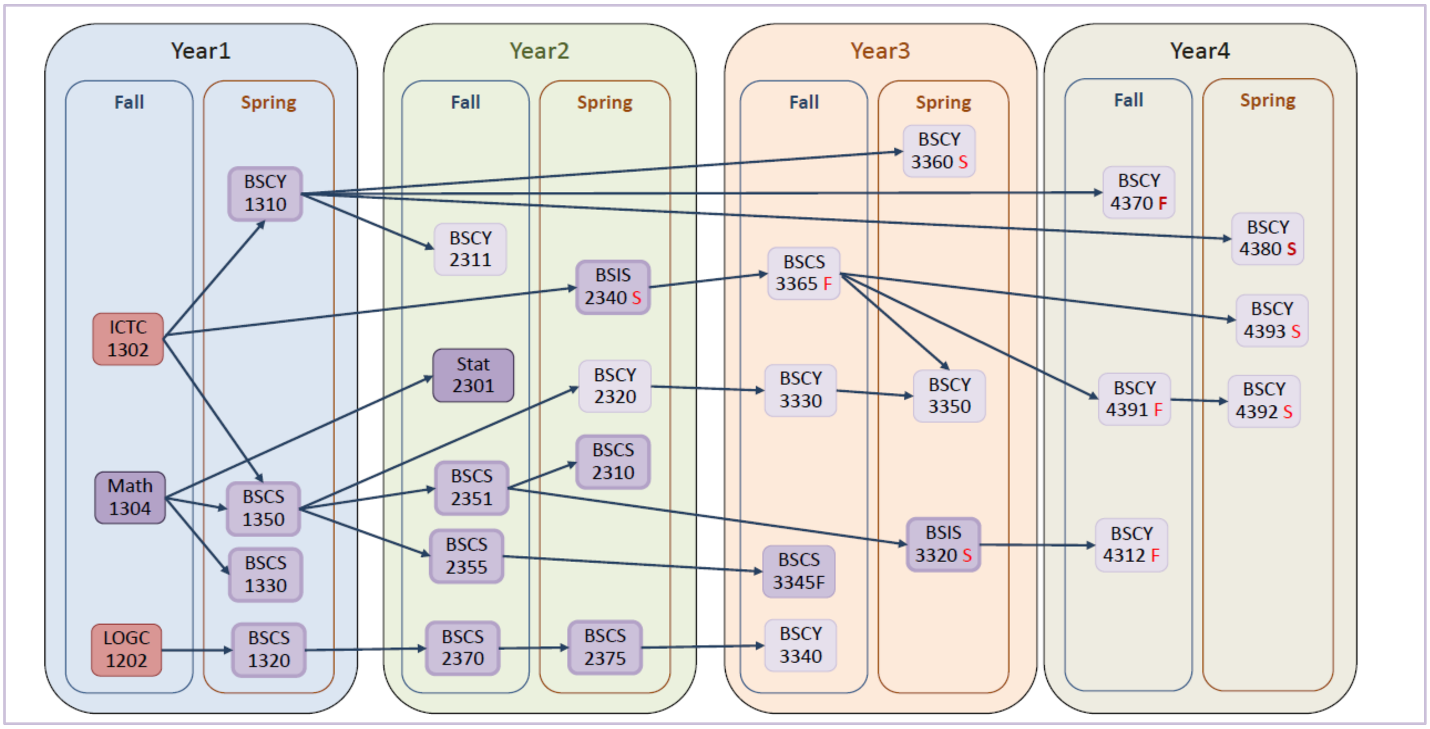
Sequence of Courses for Bachelor of Science in Cybersecurity (BCyb) Computer Forensics and Ethical Hacking Track S20-

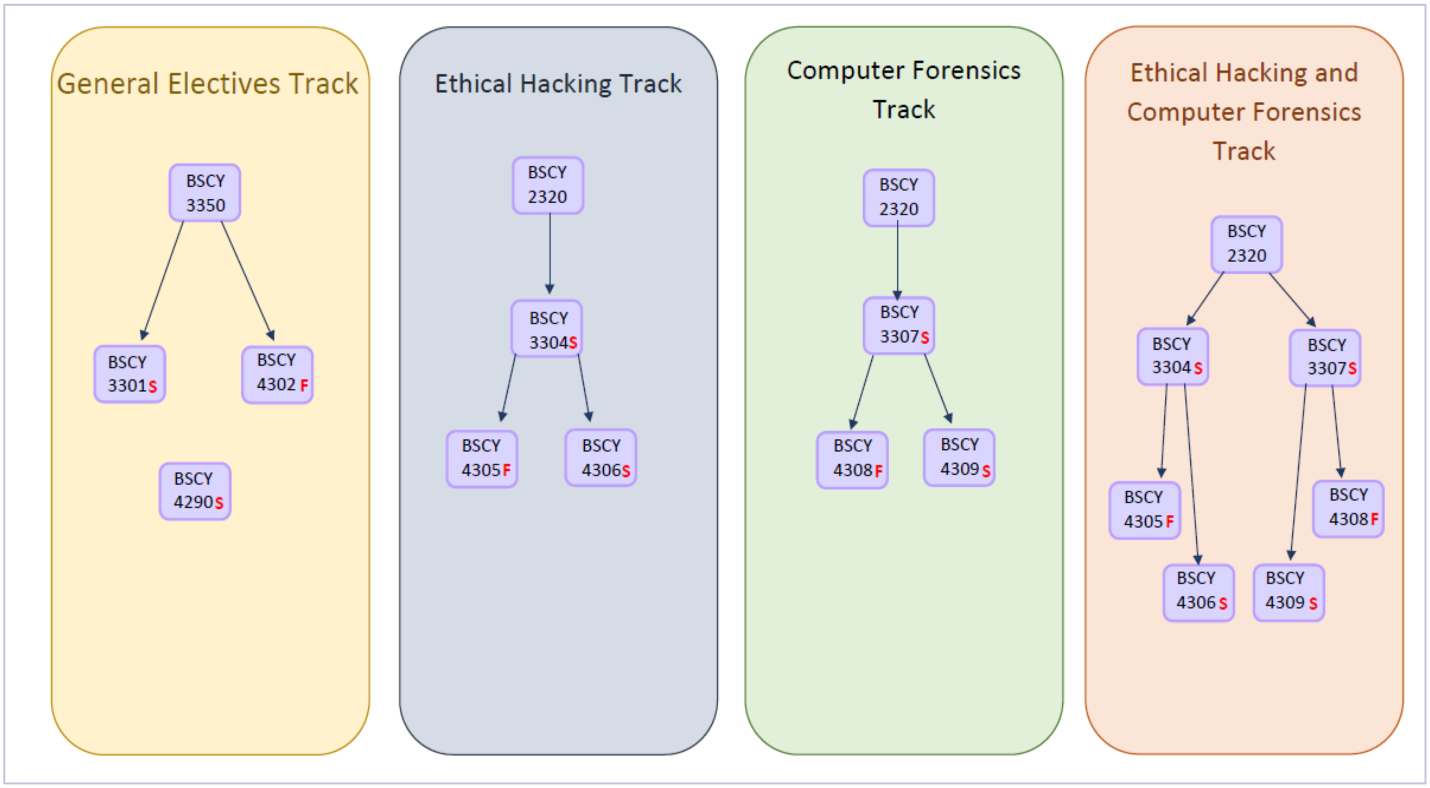
Y	S	Code	Name	CR	T
YEAR (1)	F	ICTC 1302	Information and Computing Technology Concepts	3	17
		LOGC 1202	Digital Logic Concepts	2	
		ARTS XXXX	Arts and Design	2	
		COMM 1301	Communication Skills I	3	
		ARAB XXXX	Arabic Studies	3	
		MATH 1304	Calculus I	3	
		BSCS 1160	Computer Ethics and Society	1	
	Spring	COMM 1302	Communication Skills II	3	18
		ISLS XXXX	Islamic Studies	3	
		BSCS 1330	Discrete Structures	3	
		BSCS 1350	Introduction to Programming	3	
		BSCS 1320	Computer Architecture and Organization	3	
		BSCY 1310	Fundamentals of Cybersecurity	3	
YEAR (2)	F	ISLS XXXX	Islamic Studies	3	18
		STAT 2301	Statistics	3	
		BSCS 2355	Object Oriented Programming	3	
		BSCS 2351	Fundamental Data Structures	3	
		BSCS 2370	Operating Systems	3	
		BSCY 2311	Basic Cryptography Concepts	3	
	Spring	ARAB XXXX	Arabic Studies	3	18
		XXXX XXXX	Required Gen. Ed Electives (HUMN, NASC, SBSC)	3	
		BSCS 2375	Networking and Data Communication	3	
		BSCS 2310	Analysis of Algorithms	3	
		BSIS 2340	IS Project Management	3	
		BSCY 2320	Secure Software Development	3	
YEAR (3)	F	EMOI 1201	Emotional Intelligence	2	17
		XXXX XXXX	Free Electives	3	
		BSCS 3345	Human Computer Interaction	3	
		BSCS 3365	Software Engineering	3	
		BSCY 3330	System Components Security	3	
		BSCY 3340	Networks and Connections Security	3	
	Spring	ISLS XXXX	Islamic Studies	2	17
		XXXX XXXX	Free Elective	3	
		BSIS 3320	Database Management Systems	3	
		BSCY 3350	Managing Systems Security	3	
		BSCY 3360	Human Privacy and Security	3	
		BSCY XXXX	Program Elective	3	
YEAR (4)	F	ENTR 3301	Entrepreneurship and Design Thinking	3	18
		XXXX XXXX	Required Gen. Ed Electives (HUMN, NASC, SBSC)	3	
		BSCY 4312	Information Storage Security	3	
		BSCY 4370	Organizational Risk Management and Governance	3	
		BSCY 4391	Capstone Project I	3	
		BSCY XXXX	Program Elective	3	
	Spring	BBBF 1101	Basic Body and Brain Fitness	1	13
		BSCY 4380	Societal Security and Cyber Law	3	
		BSCY 4392	Capstone Project II	3	
		BSCY 4393	Internship	3	
		BSCY XXXX	Program Elective	3	
YEAR (5)	Fall	BSCY XXXX	Program Elective	3	9
		BSCY XXXX	Program Elective	3	
		BSCY XXXX	Program Elective	3	
Total credit hours for graduation				145	145

University Requirement		19
Ministry requirement		14
Required General Elective		6
Free Elective		6
ABET (18/19V2)	Program Requirement (Math, Stat)	9
	Computing Department Requirement	34
	Program Requirement (CY Core Knowledge)	39
	Program Elective	18
Total credit hours for graduation		145

Program Electives List			
	Code	Name	CR
Electives: Ethical Hacking Track and Computer Forensics Track			
1	BSCY 3304	Ethical Hacking Concepts	3
2	BSCY 4305	Web Applications Ethical Hacking	3
3	BSCY 4306	Network Ethical Hacking	3
4	BSCY 3307	Computer Forensics Investigations	3
5	BSCY 4308	Network Forensics and Analysis	3
6	BSCY 4309	Mobile Forensics and Analysis	3

Prerequisites Tree





Course Descriptions

Course Code & Title: **BSCY 1310** **FUNDAMENTALS OF CYBERSECURITY**

Alternative Course Title: **None**

Semester Credit Hours: **3 (3, 0)**

I. Course Description:

This course introduces the concepts of cybersecurity and risk management. It highlights theimportance of cybersecurity and the integral role of cybersecurity professionals in the planning, developing, and performing security tasks and policies with respect to hardware, software, processes, networks and communications, data and applications, policies, and procedures. The course also provides the foundational cybersecurity risk management principles, including reducing vulnerabilities and threats, applying proper safeguards/controls, security architecture, compliance and operational security, threats and vulnerabilities attacks, incidents, and cryptography.

Course Code & Title: **BSCY 2311** **BASIC CRYPTOGRAPHY CONCEPTS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course introduces the essential concepts to build the base knowledge in cryptography and encryption techniques. It covers confidentiality, user authentication, data integrity, and non- repudiation. Including advanced mathematical concepts. As well as symmetric and asymmetric ciphers. The course also presents protocols and advanced protocols of cryptography.

Course Code & Title: **BSCY 2311** **BASIC CRYPTOGRAPHY CONCEPTS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course introduces the essential concepts to build the base knowledge in cryptography and encryption techniques. It covers confidentiality, user authentication, data integrity, and non- repudiation. Including advanced mathematical concepts. As well as symmetric and asymmetric ciphers. The course also presents protocols and advanced protocols of cryptography.

Course Code & Title: **BSCY 2320** **SECURE SOFTWARE DEVELOPMENT**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on fundamental principles for the implementation of security controls throughout the software development process including least privilege, open design, and abstraction concepts in the cyber context. It covers secure coding techniques and application security configuration techniques. The course also covers the roles of security requirements in the design, implementing, static and dynamic testing, configuring, and patching of software systems, as well as ethics roles, especially in development, testing and vulnerability disclosure.

Course Code & Title: **BSCY 3330** **System Components Security**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the security issues of connecting and integrating systems components and using them within larger systems. It presents security aspects of the design, fabrication, procurement, testing and analysis of systems components. The course also covers system components vulnerabilities, secure component design principles, supply chain management security, testing component security, and component reverse engineering.

Course Code & Title: **BSCY 3330** **System Components Security**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the security issues of connecting and integrating systems components and using them within larger systems. It presents security aspects of the design, fabrication, procurement, testing and analysis of systems components. The course also covers system components vulnerabilities, secure component design principles, supply chain management security, testing component security, and component reverse engineering.

Course Code & Title: BSCY 3340 Networks and Connections Security

Alternative Course Title: None

Semester Credit Hours: 3 (2, 2)

I. Course Description:

This course focuses on the security of the connections between software components including both physical and logical connections. It covers security issues, vulnerabilities, connection attacks, and Transmission attacks related to distributed systems including computer networks, World Wide Web (WWW), the Internet, High performance computing (HPC), and Cloud Services. The course also introduces current concepts in network protection including Network hardening, network traffic auditing services such as Intrusion Detection(ID) and Intrusion Prevention Services (IPS), firewalls, Virtual Private Networks (VPNs), Honeypots and honeynets, Network monitoring and traffic analysis, Network access control, Perimeter networks, Network policy and operational procedures development and enforcement as well as test the network by actually attempting to exploit vulnerabilities using session hijacking and man-in-the middle techniques.

Course Code & Title: BSCY 3350 MANAGING SYSTEMS SECURITY

Alternative Course Title: None

Semester Credit Hours: 3 (2, 2)

I. Course Description:

This course focuses on the security aspects concerning the holistic view of a software system as a complete unit in and of itself not only a set of connected components. It introduces ways for comprising security concerns through the system management including composing the system security policy, security in operation and usability considerations. The course also covers security issues related to System Access, System Control, System Retirement, and System Testing.

Course Code & Title: **BSCY 3360** **Human Privacy and Security**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the fundamental knowledge and practices for securing the data and privacy of human beings in their professional and personal life as well as studying human behavior as it relates to cybersecurity. It covers identity management methods, physical and logical assets control, users misleading, detection and mitigation of social engineering attacks (e.g. phishing, baiting ...), and system misuse and compliance with cybersecurity rules. The course also introduces Sensitive Personal Data (SPD) concept, and social media privacy and security, and human security factors.

Course Code & Title: **BSCY 4312** **Information Storage Security**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on knowledge and skills required to successfully architect, design, implement, monitor, and maintain information storage security solutions to protection data at rest, during processing, and in transit. It introduces principles of data security architecture and protection of information in computer systems including disk and file encryption in hardware- level versus software encryption. The course also covers data masking practices for testing, obfuscation, and for privacy and data erasure methods including overwriting, degaussing, physical destruction methods, and memory remanence as well as database security issues: access and authentication, auditing, and integration paradigms.

Course Code & Title: BSCY 4370 Organizational Risk Management and Governance

Alternative Course Title: None

Semester Credit Hours: 3 (2, 2)

I. Course Description:

This course focuses on fundamental knowledge and concepts concerning the organizational risk management, governance, and security policy. It introduces risk management role in the organization and methodologies for protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission. It also provides the importance, benefits, and desired outcomes of cybersecurity governance and how such a program would be implemented. The course also covers the development, implementation, and maintenance of an effective information security policy, its major types, and components as well as the role of a successful information security program.

Course Code & Title: BSCY 4380 SOCIETAL SECURITY AND CYBER LAW

Alternative Course Title: None

Semester Credit Hours: 3 (3, 0)

I. Course Description:

This course focuses on aspects of cybersecurity that affect the entire society including cybercrime, cyber law, cyber policy, cyber ethics, privacy, and their relation to each other. It covers motives of cybercrime behavior, cyber terrorism, cybercriminal investigations, economics of cybercrime, and cyber-based intellectual property theft. The course also presents legal issues and various cyber laws: privacy laws, data security law, computer hacking laws as well as cybersecurity public policy and ethical hacking issues.

Course Code & Title: **BSCY 4391** **Capstone Project I**

Alternative Course Title: **None**

Semester Credit Hours: **3 (1, 4)**

I. Course Description:

This course is part of a two-part capstone project, completed in Capstone Project II. The project stresses the integration of learning from across the curriculum within the Cybersecurity field with a strong technical focus. Teams practice gained knowledge and skills, in a realistic development setting with real clients. The course covers design thinking principles and techniques, and analysis of the client's business processes to produce a project proposal that addresses a contemporary business issue or an opportunity. Projects are completed in Capstone Project II.

Course Code & Title: **BSCY 4392** **Capstone Project II**

Alternative Course Title: **None**

Semester Credit Hours: **3 (1, 4)**

I. Course Description:

This course is a continuation of a two-part research project, begun in Capstone Project I. It stresses the integration of learning from across the curriculum within the Cybersecurity field in an applied capstone project with a strong technical focus. This course concentrates on the further development, information system project implementation, deployment and validation. The course emphasizes the successful demonstration of the information system in a practical environment.

Course Code & Title: **BSCY 4393** **INTERNSHIP**

Alternative Course Title: **None**

Semester Credit Hours: **3 (1,0, 6)**

I. Course Description:

This course offers the opportunity to undertake either an external work experience at an organization or on-site professional practicum relevant to the field of Computer Science. The Internship provides the ability to apply skills and academic knowledge acquired in a contemporary workplace situation and to receive hands-on learning, in preparation for the workforce.

Course Code & Title: **BSCY 3307** **COMPUTER FORENSICS INVESTIGATIONS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the basic computer forensics knowledge and skills needed by analysts and incident responders to identify and counter a wide range of threats within enterprise networks, including economic espionage, hacktivism, and financial crime syndicates. It introduces definitions, limits, and types of digital forensics tools and the investigatory process stages: acquisition and preservation of evidence, evidence analysis, results presentation, and evidence authentication. The course also covers the methodology for reporting, investigating, responding, and handling of computer incidents as well as collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation.

Course Code & Title: **BSCY 4308** **NETWORK FORENSICS AND ANALYSIS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the skills needed to mount efficient and effective post-incident response investigations. It introduces the tools, technology, and processes required to integrate network evidence sources into investigations, covering high-level NetFlow analysis, low-level pcap exploration, and ancillary network log examination. The course also covers a wide range of open source and commercial tools, and real-world scenarios to learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

Course Code & Title: **BSCY 4309** **MOBILE FORENSICS AND ANALYSIS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on the mobile forensics knowledge and skills to perform forensic examinations on devices such as mobile phones and tablets. It introduces device file system analysis, mobile application behavior, event artifact analysis, and the identification and analysis of mobile device malware. The course also covers the needed forensic tools and custom scripts to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices.

Course Code & Title: **BSCY 3304** **Ethical Hacking Concepts**

Alternative Course Title: **None**

Semester Credit Hours: **3 (2, 2)**

I. Course Description:

This course focuses on hacking tools, techniques, exploits, and the critical activity of incident handling by adopting the viewpoint of a hacker. It introduces an entirely different way of achieving optimal information security posture in organizations through ethical hacking principle to scan, test, hack, and secure their systems.

Course Code & Title: BSCY 4305 WEB APPLICATIONS ETHICAL HACKING

Alternative Course Title: None

Semester Credit Hours: 3 (2, 2)

I. Course Description:

This course focuses on inner mechanisms of web applications and how these applications can be broken, analyzed, and penetrated. It introduces all vulnerability classes pertaining to web applications, and how each vulnerability class can be discovered, attacked, and mitigated. It also covers the concepts, skills, and tools for Cross-Site Scripting (XSS) attacks, Cross-Site Request Forgery (CSRF) attacks, SQL Injection (SQLi) attacks, file inclusion attacks, command execution attacks, and many others.

Course Code & Title: BSCY 4306 NETWORK ETHICAL HACKING

Alternative Course Title: None

Semester Credit Hours: 3 (2, 2)

I. Course Description:

This course focuses on conducting successful penetration testing and ethical hacking for computer networks. It introduces the steps of pen testing planning, scoping, and reconnaissance. The course also covers target environment scanning tools, kinds of exploits used to compromise target machines including client-side exploits, service-side exploits, and local privilege escalation, and performing post-exploitation and pivoting as well as password cracking and attacks.

Course Code & Title: **BSCY 3301** **IT AUDIT AND CONTROLS**

Alternative Course Title: **None**

Semester Credit Hours: **3 (3, 0)**

I. **Course Description:**

This course presents the essential principles of the information technology audit and control function. It defines the information controls, their kinds, and their effects on the organization and explains how to manage and audit them using concepts and techniques of information technology audits. It covers the process of creating a control structure with goals and objectives, audit of an information technology infrastructure, and systematic remediation procedures for improvements. The course also focuses on audit and control best practices, standards, and regulatory requirements governing information.

Course Code & Title: **BSCY 3302** **EMERGING TECHNOLOGIES IN CYBERSECURITY**

Alternative Course Title: **None**

Semester Credit Hours: **3 (3, 0)**

I. **Course Description:**

This course provides an overview of theory and practice related to contemporary topics in cybersecurity, including emerging technologies, new trends, and policies. It covers how emerging trends in cybersecurity can be analyzed and reviewed to be adopted by organizations to provide competitive advantages in the workplace. This course also evaluates how policies and procedures continue to evolve as technology changes and become more capable in the workplace.

Course Code & Title: BSCY 3390 RESEARCH METHODS IN CYBERSECURITY

Alternative Course Title: None

Semester Credit Hours: 3 (3, 0)

I. Course Description:

The course enhances the knowledge of research methods on both practical and theoretical level, including lectures and seminars. It explains various research methods and techniques within the area of Cybersecurity (CY). It also covers planning, designing, and carrying out investigations and studies using both qualitative and quantitative methods in addition to writing up and presenting the research reports and results.

Certificates:

EC-Council

- Computer Hacking Forensic Investigator (CHFI)
- Certified Ethical Hacker (CEH)
- Certified Encryption Specialist

CISCO

- Introduction to Cybersecurity
- Network Security
- CCNA Introduction to Networks

Program Committees' Membership

Committees	Members	Meeting Schedule
BCyb Department Council	**Chairperson:** Dr. Sahar Shabanah, BCyb Acting Director **Members:** Dr. Saoucene Mahfodh, BCS Director Dr. Louai Maghrabi, Assistant Professor Dr. Dheyaaldin Salman, Assistant Professor Ms. Laila Abuljadayel, Lecturer	**Fall 2021-2022** August 30, 2021 September 28, 2021 October 26, 2021 November 30, 2021 December 28, 2021 **Spring 2021-2022** January 24, 2022 February 28, 2022 March 22, 2022 April 19, 2022 May 10, 2022
BCyb Department Curriculum Committee	**Chairperson:** Dr. Sahar Shabanah, BCyb Acting Director **Members:** Dr. Saoucene Mahfodh, BCS Director Dr. Louai Maghrabi, Assistant Professor Dr. Dheyaaldin Salman, Assistant Professor Ms. Laila Abuljadayel, Lecturer	**Fall 2021-2022** August 29, 2021 September 27, 2021 October 27, 2021 November 29, 2021 December 27, 2021 **Spring 2021-2022** January 23, 2022 February 27, 2022 March 23, 2022 April 18, 2022 May 09, 2022

BCyb Department Examination Committee	**Chairperson:** Dr. Sahar Shabanah, BCyb Acting Director **Members:** Dr. Saoucene Mahfodh, BCS Director Dr. Louai Maghrabi, Assistant Professor Dr. Dheyaaldin Salman, Assistant Professor Ms. Laila Abuljadayel, Lecturer	**Fall 2021-2022** October 03, 2021 December 12, 2021 **Spring 2021-2022** February 20, 2022 May 15, 2022
BCyb Department Advisory Committee	**Chairperson:** Dr. Sahar Shabanah, BCyb Acting Director **DAH Members:** Dr. Louai Maghrabi, Assistant Professor Dr. Dheyaaldin Salman, Assistant Professor Ms. Laila Abuljadayel, Lecturer **External Members:** Dr. Ehab Abozinada, Vice Dean at KAU Eng. Doaa Zamzami, Engineer at Saudi Aramco Ms. Shahad Attar, Director at STC Hashem Aidaros, Assistant Professor at Alfaisal University Dr. Saoucene Mahfodh, Assistant Professor Mr. Mohammed Almmintakh, Cybersecurity Consultant, Threat Intelligence at Mobily, Riyadh **Alumani:** Mawaddah Mirza – BCyb Senior Student	**Fall 2021-2022** September 20, 2021 **Spring 2021-2022** February 21, 2022

Internship Guide

Introduction

The purpose of the Internship is to offer the opportunity to undertake either an external work experience at an organization or on-site professional practicum relevant to the field of Cybersecurity. The Internship provides the ability to apply skills and academic knowledge acquired in a contemporary workplace situation and to receive hands-on learning, in preparation for the future career life.

Learning Objectives

The Internship is one of the most useful areas for students to achieve the program student outcomes determined by ABET Accreditation for the cybersecurity program. Hence, by the end of the internship, the student should be able to:

1. Identify career opportunities, interests and abilities in different fields of cybersecurity prior to graduation.

2. Identify curriculum courses that their knowledge has been applied in the field experience.

3. Apply different cybersecurity theory and practices to solve real-life problems in field experience.

4. Communicate effectively in written and thorough oral forms within the work environment.

5. Engage in problem solving and critical thinking tasks.

6. Complete the tasks assigned in the job as required.

7. Acquire job interview and CV writing skills to increase employment opportunitiesfollowing graduation.

8. Exhibit time management, teamwork and professional skills.

9. Comply with work ethics and code of conducts.

10. Exhibit interpersonal skills and professional attitudes within the work environment.

ABET Outcomes

11. Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

12. Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program’s discipline.

13. Communicate effectively in a variety of professional contexts.

14. Recognize professional responsibilities and make informed judgements in computing practice based on legal and ethical principles.

15. Function effectively as a member or leader of a team engaged in activities appropriate to the program’s discipline.

16. Apply security principles and practices to maintain operations in the presence of risks and threats.

Internship Areas

Before being permitted to apply for internship, student should demonstrate their good understanding of the area in which training has to be pursued. The student area of training should be directly related to the program degree, that is any areas within cybersecurity (i.e., data security, software security, component security, connection security, system security, human security, organizational security and societal security and/or other related areas) in any recognized governmental or private sector in organizations, ministries, companies, corporations, agencies, etc.

Duration Requirements

The student should fulfil the following minimum requirements for internship duration:

- Number of weeks: 12 weeks
- Number of days: 90 days
- Number of hours: 400 hours

Once a student has joined a particular internship site, the student will ensure completion of internship duration as stated above and does not transfer to any other site. In the caseof non-compliance with the minimum duration of internship, the student trainee will not pass in the course and will have to register again.

Internship Planning and Structure

Eligibility & Registration Process

The following criteria should be met before a student is considered eligible for Internship:

1. The student has to complete all prerequisite courses and a minimum of 90 credit hours after the preparatory year prior to registering for the Internship.

2. The student must be an active registered student of the degree program to be ableto apply for internship.

3. Student is not permitted to register for any other courses during the internship.

Attendance Requirements

The attendance ratio should be greater than 90%. Failure to achieve the minimum attendance requirement will result in failing the internship.

Approval Process

Before the commencement of internship semester, the eligible student is responsible for browsing appropriate and relevant internship opportunities and contacting the internship site to get accepted in an internship program.

Once accepted in an internship program, the student should fill in the Internship Agreement form (Form (1)) with their site supervisor. The form should be sent to the student’s assigned university internship advisor no later than one week from the internship start date to be approved or rejected by the internship assigned committee.

During Internship

Once approved, the student can start the internship and will have to document the performed tasks and fill in a monthly report form (Form (2)) for each internship month. The report should be signed and stamped by the internship supervisor, and submitted at the end of the internship.

During the training period, the student is responsible for abiding by and complying with all the rules, regulations and professional ethics of the internship site. The student trainee should comply with the training commitments stated in the internship instructions, otherwise; the student grade will be affected. It is also the responsibility of student to promptly notify any changes to the internship plan or supervisor and refill required forms.

ce the student is eligible, she is expected to register for the internship through SIS

After the Internship

Upon completion of the internship, it is the student's responsibility to make sure that the following forms are submitted as hard-copy and via email within 7 days after the end of the internship program:

4. Site Evaluation of student (Form (3)): The form will be sent to the site supervisor to evaluate the student's performance.

5. Student Internship Evaluation (Form (4)): The form will be sent to the student to evaluate the internship site.

6. Internship Indirect Assessment (Form (5)): The form will be sent to the student to evaluate their own performance against internship Course Learning Outcomes.

After submission of all required forms, the student then will have to appear for an interview with the internship committee. The committee will determine the overall performance of the student and recommend for No Grade-Pass or No Grade-Fail grade.

Grading

The internship will be graded as No Grade-Pass or No Grade-Fail.
If the student fails to fulfill any of the requirements mentioned above, she will fail the course and will be graded (NF: Nograde – Fail). The student may fall in one of the following categories:

- If the student does not fulfill the attendance rate required, he/she should re-register for the internship.

- If the student does not score the minimum score in organization evaluation, he/she should repeat the training course.

- If the student does not score the minimum score in the final report, he/she should resubmit another report within a time line not exceeding two working weeks fromthe announcement of results for the practical training course.

- If the student fails to appear for the final interview or is unable to pass the interview.

Special Cases

Students are eligible to transfer from the internship site no later than one week from the starting date of the internship. The student should fill in and re-submit a new Internship Agreement form (Form (1)) to the internship committee no later than three days before she leaves the training organization. The submitted form is subject to approval conditioned by the provision of alternative internship site by the student herself, willing to train her during the semester she has applied for the internship. The student will be held responsible for her negligence, which will entail failure in the course.

Contact Us:

The Dean of HECI	**Phone**	**Email**
Dr. Sahar Shabanah	966-12-630-3333 EXT#392	sshabanah@dah.edu.sa
Admin of the Program	**Phone**	**Email**
Ms. Eman Bakhashwain	966-12-630-3333 EXT# 268	ebakhashwain@dah.edu.sa

For more information, please visit DAH website:

Follow us on social media accounts:@ DAHUniversity

dahuniversity , heci_dah