College of Computing and Informatics

STUDY PLAN PROJECT

MASTER OF CYBER SECURITY

September 2023

Introduction

The College of Computing and Informatics at the Saudi Electronic University offers a master's program in cybersecurity, which aims to provide students with advanced knowledge necessary to excel in the contemporary highly competitive technology industry. The program focuses on the security of the institution's cyberspace. The program equips students with the knowledge, skills and capacity to prevent and protect enterprise data from the threat of various forms of digital crime. The courses also focus on critical analysis skills, technical skills and extensive use of virtual laboratories via the Internet. This program is designed for students wishing to pursue their careers as specialists in information technology with the aim of protecting the information of their institutions from any external penetration by integrating theories with practical application. To know the basics of information systems and know how to manage information technology within the framework of the fundamentals of cybercrime. The program covers the field of security and legal aspects that affect information security in cyberspace.

The Importance and Reasons for Creating the Program

- Keeping pace with the needs of the labor market and the Kingdom's 2030 vision.
- The need for qualified professionals with the necessary knowledge and skills in the field of cybersecurity.
- The need for qualified specialists in the field of combating electronic information crimes.
- The need for specialists in assessing and analyzing local and international breaches that may occur to information systems.
- The need for specialists with the ability to know the various vulnerabilities of computer networks and the methods used to penetrate network security and provide comprehensive solutions to reduce these breaches.

Program Objectives

1. Provide experts in the field of cybersecurity to perform innovative research in cybersecurity and help achieving the kingdom long term plan of having experts in the field of cybersecurity.
2. Empower students with soft skills and values to effectively communicate and collaborate with others professionally, ethically, legally and serve society's requirements.

3. Ensure the knowledge and skills of students are in line with state-of-the-art cybersecurity techniques.

Duration of Study in the Program

4 semesters, 36 credit hours (12 courses).

Program Learning Outcomes

1. Explain in detail various cybersecurity models, their capabilities, structure, strengths and weaknesses; and the risks associated with transferring and storing information assets in global organizations.
2. Critically demonstrate state-of-the-art solutions to protect information assets from internal and external threats, risks and intrusions.
3. Analyze various strengths and weaknesses of IT networks and their vulnerabilities to both internal and external threats and intrusions.
4. Develop and evaluate the best cybersecurity practices and solutions for protecting the Internet and information networks from internal attacks, external cyber-attacks, and intrusions.
5. Demonstrate the application of effective teamwork, oral and written communication, and research skills.
6. Provide advanced solutions to ethical and legal issues related to use of Cybersecurity in local and global environments.

Career Opportunities for Graduates of the Program

At the end of the program, students will be prepared for the following professions and occupations:

- Project Manager.
- Information Security Analyst.
- Cyber Security Manager.
- Cyber Security Analyst.
- Information Security Manager.
- Information Technology Manager.
- Network Security Manager.
- Network Security Analyst.
- Educational and academic field occupations in general and higher education institutions

Vision

Prepare qualified and skilled students to meet the needs of the labor market in the field of Cybersecurity and to pursue advanced degrees; by providing outstanding education with state-of-the-art concepts, knowledge, practical techniques and research skills in Cybersecurity.

Mission

Providing high-quality and flexible educational, scientific and research environment in the field of Cybersecurity to supply the labor market with qualified cybersecurity experts capable of performing professional services and producing innovative scientific research that contributes to the development of a knowledge society, meeting international requirements, solving community problems and facing future challenges in Cybersecurity.

Program Study Plan

The Master of Cyber Security program contains 12 courses, distributed over 4 semesters.The program is only offered in English.

University Requirements: (3 Credits)

1. CYS501: Research Methods in Computational Studies

College Requitements: (0 Credits)

N.A.

Specialization Requirements: (33 Credits)

1. CYS507: Introduction to Cyber Security and Digital Crime
2. CYS512: Cryptography Fundamentals
3. CYS564: Cyber Defense in Web Based Attacks
4. CYS566: Securing Enterprise Infrastructure using Cyber Security Techniques
5. CYS663: Digital Forensics and Investigations
6. CYS613: Security Threats and Countermeasures in Complex Organizational Networks
7. CYS645: Information Security Management, Legal and Ethical Issues
8. CYS642: Innovative Solutions in Software Security
9. CYS683: Ethical Hacking and Penetration Testing
10. CYS666: Advanced Principles of Cyber Security
11. CYS698: Capstone Project in Cyber Security

Electives: N.A.

Program Structure

#	Course Code	Course Title	Credit hours	Pre-requisites
1	CYS501	Research Methods in Computational Studies	3	-
2	CYS507	Introduction to Cyber Security and Digital Crime	3	-
3	CYS512	Cryptography Fundamentals	3	-
4	CYS564	Cyber Defense in Web Based Attacks	3	CYS507
5	CYS566	Securing Enterprise Infrastructure using Cyber Security Techniques	3	CYS507
6	CYS663	Digital Forensics and Investigations	3	CYS507
7	CYS613	Security Threats and Countermeasures in Complex Organizational Networks	3	CYS564
8	CYS642	Innovative Solutions in Software Security	3	CYS566
9	CYS645	Information Security Management, Legal and Ethical Issues	3	CYS507
10	CYS666	Advanced Principles of Cyber Security	3	CYS566
11	CYS683	Ethical Hacking and Penetration Testing	3	CYS645
12	CYS698	Capstone Project in Cyber Security	3	CYS501 + Department Approval
Total Credits			36	

Program Structure by Levels

Level One

#	Course Code	Course Title	Credit Hours	Pre-Requisites
1	CYS501	Research Methods in Computational Studies	3	-
2	CYS507	Introduction to Cyber Security and Digital Crime	3	-
3	CYS512	Cryptography Fundamentals	3	-

Level Two

#	Course Code	Course Title	Credit Hours	Pre-Requisites
1	CYS564	Cyber Defense in Web Based Attacks	3	CYS507
2	CYS566	Securing Enterprise Infrastructure using Cyber Security Techniques	3	CYS507
3	CYS663	Digital Forensics and Investigations	3	CYS507

Level Three

#	Course Code	Course Title	Credit Hours	Pre-Requisites
1	CYS613	Security Threats and Countermeasures in Complex Organizational Networks	3	CYS564
2	CYS642	Innovative Solutions in Software Security	3	CYS566
3	CYS645	Information Security Management, Legal and Ethical Issues	3	CYS507

Level Four

#	Course Code	Course Title	Credit Hours	Pre-Requisites
1	CYS666	Advanced Principles of Cyber Security	3	CYS566
2	CYS683	Ethical Hacking and Penetration Testing	3	CYS645
3	CYS698	Capstone Project in Cyber Security	3	CYS501 + Department Approval

Program Courses Descriptions

List all courses here following this format:

Course Title	Research Methods in Computational Studies
Course Code	CYS501
Pre-requisite(s)	-
Credit hours	3
Contact hours	3
Course Description	This course provides an overview of the important concepts of research design, data collection, statistical and interpretative analysis, and final report presentation. The focus of this course is not on mastery of statistics but on the ability to use research in Computational Studies. Students will prepare a preliminary research design for projects in their subject matter areas and how to accurately collect, analyze and report data. Students will focus on the steps needed to design an individual research project or thesis. The course provides real world active learning assignments that seek to integrate the Knowledge and skills gained through undergraduate course work. The course focuses on scientific writing, and oral, written, and graphical presentation of data and research results.

Course Title	Introduction to Cyber Security and Digital Crime
Course Code	CYS507
Pre-requisite(s)	-
Credit hours	3
Contact hours	3

Course Description	This course provides an introduction to cyber security and digital crime. Students will learn about cyber security threats, dangers, and risks that organizations face and will develop the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.

Course Title	Cryptography Fundamentals
Course Code	CYS512
Pre-requisite(s)	-
Credit hours	3
Contact hours	3
Course Description	This course provides students with a thorough review of cryptography and cryptographic techniques as they apply to the area of information and computer security. Students will learn about various cryptography techniques along with their advantages and disadvantages. Additionally, discussion will be provided on the various systems that are used to provide secure and encrypted end-to-end communications to include: pre- shared keys, hashing algorithms, certificates, public-key/private key infrastructures and shared secret keys.

Course Title	Cyber Defense in Web Based Attacks
Course Code	CYS564
Pre-requisite(s)	CYS507
Credit hours	3
Contact hours	3

Course Description	This course includes a focus on external cyber security threats including the Internet, information networks and the World-Wide Web. There will be a detailed view into social media, search engines, and current trends that integrate social media outlets into the enterprise as a means of achieving strategic objectives. Risk mitigation and SQL injection prevention techniques will also be discussed.

Course Title	Securing Enterprise Infrastructure using Cyber Security Techniques
Course Code	CYS566
Pre-requisite(s)	CYS507
Credit hours	3
Contact hours	3
Course Description	The course reinforces cyber security methods in critical infrastructures equipping students with the knowledge and hands-on experience of protecting large Windows Based infrastructure services. Students will also gain insight into complex cyber security system design, deployment, and ongoing maintenance. Holistic security techniques will be covered to provide complete system and enterprise security. Patch management and vulnerability detection for Windows-based systems is also discussed.

Course Title	Digital Forensics and Investigations

Course Code	CYS663
Pre-requisite(s)	CYS507
Credit hours	3
Contact hours	3
Course Description	This course provides students with insight to system forensics investigation and response. Areas of study include procedures for investigating computer and cybercrime, and concepts for collecting, analyzing, recovering, and preserving forensic evidence. Students will learn how to respond to cyber breaches, including the recovery, preservation, analysis of digital evidence, and proper incident response. In addition to the tools of the digital forensics trade, students will become familiar with relevant federal statutes. They will be presented with various scenarios a digital forensics investigator may face and be asked how they would react.

Course Title	Security Threats and Countermeasures in Complex Organizational Networks
Course Code	CYS613
Pre-requisite(s)	CYS564
Credit hours	3
Contact hours	3

Course Description	The course details different network infrastructure security threats, attacks, and countermeasures at different organizational network layers. It includes perimeter security defenses, firewalls, virtual private networks, intrusion detection systems, wireless security, mobile networks, and network security auditing tools.

Course Title	Innovative Solutions in Software Security
Course Code	CYS642
Pre-requisite(s)	CYS566
Credit hours	3
Contact hours	3
Course Description	This course discusses how to construct secure innovative programs. The course explores secure software development through the use of secure coding, program analysis, and advanced testing. The course details secure programming techniques to defend against source code software vulnerabilities such as overwriting, buffer overflow, and code injection. The overview is given for secure web application development against web attacks such as SQL injection, Cross-Site Scripting (XSS), secure session management, and secure authentication.

Course Title	Information Security Management, Legal and Ethical Issues

Course Code	CYS645
Pre-requisite(s)	CYS507
Credit hours	3
Contact hours	3
Course Description	In this course, students will examine how law, ethics, and technology intersect in organizations that rely on information technology. Students will gain an understanding and insight into issues arising from privacy, secrecy, access control, and policy enforcement, as well as other legal and ethical dilemmas prevalent in today's organizations.

Course Title	Advanced Principles of Cyber Security
Course Code	CYS666
Pre-requisite(s)	CYS566
Credit hours	3
Contact hours	3
Course Description	This course provides students with an overview of cyber security access control to protect resources against unauthorized viewing, tampering, or destruction to ensure privacy, confidentiality, and prevention of unauthorized disclosure. Access Control, Authentication, and Public Key Infrastructure define the components of access control, provide a business framework for implementation, and discuss legal requirements that impact access control programs. The course looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them.

Course Title	Ethical Hacking and Penetration Testing
Course Code	CYS683
Pre-requisite(s)	CYS645
Credit hours	3
Contact hours	3
Course Description	This course provides students with the knowledge and practice needed to secure information systems against attacks such as viruses, worms, and other system weaknesses that pose significant danger to organizational data. Ethical hacking and penetration testing are applied to uncover common techniques used by cyber criminals to exploit system vulnerabilities.

Course Title	Capstone Project in Cyber Security
Course Code	CYS698
Pre-requisite(s)	CYS501 + Department Approval
Credit hours	3
Contact hours	3

Course Description	In the capstone project, students explore the literature, conduct research and develop solutions to help analyze organizations security needs related to continuously evolving security challenges. Students will analyze organizational objectives and propose solution(s) and implementation plan(s). The proposed solution must address strategies to overcome challenges of cyber security related projects such as assessing risks, reduction of fund, and keeping the support of executive management. Students will utilize skills gained throughout the program to demonstrate the ability to design a cyber security project from conception to publishing/deployment.