



ABDULLAH AL SALEM UNIVERSITY (AASU)

Graduate Academic Programs

Cybersecurity Engineering

2025/2026

Version 1.1

Table of Contents

<i>General Introduction.....</i>	<i>3</i>
<i>The Vision.....</i>	<i>3</i>
<i>The Mission</i>	<i>4</i>
<i>Programs' Development.....</i>	<i>4</i>
<i>Graduate Attributes</i>	<i>4</i>
<i>College of Computer & Systems Engineering.....</i>	<i>5</i>
<i>Cybersecurity Engineering</i>	<i>6</i>
<i>Program Overview</i>	<i>6</i>
<i>Program Objectives.....</i>	<i>6</i>
<i>Program Requirements.....</i>	<i>6</i>
<i>Course Descriptions</i>	<i>8</i>
<i>College of Computer & Systems Engineering</i>	<i>8</i>

General Introduction

Abdullah Al-Salem University (AASU) proudly offers Master's programs that align closely with Kuwait's Vision 2035, across three distinguished colleges: the College of Engineering and Energy, the College of Computing & Systems, and the College of Business and Entrepreneurship. Rooted in a tradition of academic excellence and driven by a commitment to innovation, these programs are designed to equip students with the knowledge, skills, and experience needed to excel in their chosen fields.

In the College of Engineering and Energy, students engage in rigorous coursework and groundbreaking research, guided by esteemed faculty members who are experts in their respective disciplines. With access to state-of-the-art laboratories and research facilities, students have the opportunity to explore emerging technologies and tackle complex engineering challenges. From renewable energy to sustainable infrastructure, graduates emerge prepared to lead the way in shaping the future of engineering and energy solutions.

Meanwhile, in the College of Computer & Systems Engineering, Abdullah Al-Salem University empowers students to thrive in the digital age. Through a blend of theoretical instruction and hands-on practice, students delve into the latest advancements in computer science, artificial intelligence, and information systems. With access to cutting-edge computing facilities and research centers, students collaborate with faculty members on innovative research projects and gain valuable industry insights. Graduates emerge with the skills and expertise to drive technological innovation and address the complex challenges of our interconnected world.

In the College of Business and Entrepreneurship, Abdullah Al-Salem University fosters a culture of creativity, innovation, and enterprise. Our Master's programs provide students with a comprehensive understanding of business principles, coupled with practical experience and real-world application. Through internships, case studies, and entrepreneurial projects, students develop the skills needed to thrive in a competitive business environment. With access to cutting-edge research centers and entrepreneurial incubators, graduates emerge as agile thinkers and visionary leaders, prepared to make a lasting impact in the global marketplace.

The Vision

AASU shall be an institution of choice that will contribute to the socio-economic development of Kuwait by promoting innovation in education, world-class research, creativity, and entrepreneurship.

The Mission

To establish strong and balanced academic programs, research, and outreach programs, that contribute to the development and advancement of Kuwait and the region.

Programs' Development

AASU has meticulously crafted its academic programs in accordance with the comprehensive framework portrayed by Kuwait Vision 2035. These programs are tailored to meet the dynamic demands of the contemporary job market, informed by extensive research conducted by prominent institutions such as the Supreme Council for Planning and Development (SCPD), the Kuwait Foundation for the Advancement of Sciences (KFAS), and the World Bank. Moreover, the university has conducted thorough analyses of requisite skill sets for the workforce, drawing insights from research conducted by the Kuwait Institute for Scientific Research (KISR) and consultations with key stakeholders from both the public and private sectors.

The curriculum of AASU's programs is enriched by a diverse range of specializations, fostering a multidisciplinary approach that aligns with Kuwait's broader educational objectives. Furthermore, the university is committed to enhancing its regional and global presence within academic circles. Through these concerted efforts, Abdullah Al-Salem University ensures that its programs are not only forward-thinking but also responsive to the evolving needs of the modern world.

Graduate Attributes

AASU is dedicated to cultivating the following set of attributes that empower graduates to excel in their academic pursuits and thrive in their professional endeavors:

- Job-ready professionals who can quickly contribute to their workplace by applying acquired core concepts and skills to relevant job fields.
- Creative thinkers and problem solvers who can use their intellectual curiosity and critical thinking to find sustainable solutions to complex, real-life problems.
- Effective collaborators who can communicate professionally, adapt, debate, and act as team players.
- Entrepreneurial individuals who can identify an opportunity and transform concepts into reality.
- Responsible global citizens and lifelong learners who can act in a manner that promotes professionalism, ethical behavior, accountability, and social responsibility, and engage in a self-motivated pursuit of knowledge for either personal fulfillment or professional growth.

College of Computer & Systems Engineering

Graduating with a Master of Science (M.Sc.) in this field necessitates the successful completion of a total of 33 credit hours (CHs). These credit hours are distributed across university, college, and program requirements, encompassing courses that are essential as well as those that can be chosen based on stream preference.

The 33 credit hours are distributed as follows:

- 6 CHs: College requirements (Table 1).
- 9 CHs: Thesis work. (Table 2).
- 9 CHs: Program requirements (Table 3).
- 9 CHs: Program electives (Table 4).

* Thesis defense must be passed before graduation according to working regulations.

* Based on the qualifications of the admitted applicants, additional coursework might be suggested in addition to the program requirements if deemed necessary by the program scientific committee.

Table 1 below shows the list of college requirements courses for the graduate programs at AASU:

Table 1: College requirement coursework (6 CHs).

Course Code	Course Title	Credit hours	Contact hours	Pre-requisite	Co-requisite
CCS501	Analysis and Design of Algorithms	(3 credits)	3		
CCS502	Scientific Research Methods	(3 credits)	3		

Table 2 below shows the list of the thesis requirements for the graduate programs at AASU:

Table 2: Thesis requirements for Graduate Programs at AASU (9 CHs).

Course Code	Course Title	Credit hours	Contact hours	Pre-requisite	Co-requisite
CSE697	Thesis Proposal	(3 credits)	Not specified	Completion of at least 6 credits with a GPA of 2.67 or higher.	CCS502
CSE698	Thesis Continuation	(0 credits)	Not specified	CSE697	
CSE699	Thesis	(6 credits)	Not specified	CSE697 OR CSE698	

Cybersecurity Engineering

Program Overview

The Master of Science in Cybersecurity Engineering Program at AASU is a specialized graduate program designed to equip students with the essential skills and knowledge to navigate the complex landscape of cybersecurity. Through a blend of theoretical foundations and practical applications, students delve into areas such as cryptography, network security, artificial intelligence-based measures, and risk management. The program emphasizes hands-on experience and real-world projects, preparing graduates to tackle emerging cyber threats and safeguard digital assets. With access to cutting-edge resources and industry partnerships, students emerge as skilled cybersecurity professionals, ready to address the evolving challenges of the digital age.

Program Objectives

- a. Equip students with comprehensive knowledge and skills in cybersecurity principles, techniques, and technologies.
- b. Integrate machine learning concepts into cybersecurity practices to enhance threat detection and mitigation strategies.
- c. Provide hands-on experience through practical projects and real-world simulations to develop practical cybersecurity skills.
- d. Foster critical thinking and problem-solving abilities to address evolving cybersecurity threats effectively.
- e. Prepare graduates to assume leadership roles in cybersecurity management and contribute to the protection of digital assets in various sectors.
- f. Cultivate a deep understanding of ethical considerations and legal frameworks relevant to cybersecurity practices.
- g. Prepare graduates to obtain industry-recognized certifications such as CISSP, CEH, or CompTIA Security+.

Program Requirements

Table 3 below shows the list program course requirements (9 credits) for the graduate programs at AASU in cybersecurity. With pre-approval from their advisors, students are required to select a minimum of 9 credits from the program's elective coursework, as outlined in Table 4. Additionally, they have the option (with the advisor's pre-approval) to take up to 6 credits from those 9 credits from other programs within the university to fulfill graduation requirements.

Table 3: Program coursework (9 CHs).

Course Code	Course Title	Credit hours	Contact hours	Pre-requisite	Co-requisite
CSE501	Cybersecurity Engineering	(3 credits)	3		
CSE502	Cybersecurity Models and Laws	(3 credits)	3		
CSE503	Game Theoretic Modeling	(3 credits)	3		

Table 4: Program Electives (9 CHs).

Course Code	Course Title	Credit hours	Contact hours	Pre-requisite	Co-requisite
CSE504	Cybersecurity Governance and Risk Management	(3 credits)	3	CSE502	
CSE505	Distributed Networks Security	(3 credits)	3	CSE501	
CSE506	Machine Learning for Cybersecurity	(3 credits)	3	CSE501	
CSE507	IoT applications and Security	(3 credits)	3	CSE501	
CSE601	Secure Cloud Computing and Virtualization	(3 credits)	3	CSE501	
CSE602	Cyber Threats and Defense Strategies	(3 credits)	3	CSE502	
CSE603	Ethical Hacking and Penetration Testing	(3 credits)	3	CSE501	
CSE604	Blockchain Technology and Cryptocurrency Security	(3 credits)	3	CSE501	
CSE605	Secure Software Development and Code Analysis	(3 credits)	3	CSE501	
CSE606	Advanced Cryptography and Security	(3 credits)	3	CSE501	
CSE607	Incident Response and Digital Forensics	(3 credits)	3	CSE501	
CSE608	Advanced Topics in Cybersecurity	(3 credits)	3	CSE501	

Course Descriptions

College of Computer & Systems Engineering

Course Code: CCS501

Course Title: Analysis and Design of Algorithms

Course Prerequisite: None

Course Co-requisite: None

Course Description: This course delves into advanced techniques for designing and analyzing algorithms to solve complex computational problems efficiently. Topics include advanced data structures, graph algorithms, dynamic programming, greedy algorithms, and approximation algorithms. Emphasis is placed on computational complexity, algorithm optimization, and real-world applications. Students will gain hands-on experience in evaluating algorithm performance and developing solutions for challenging problems, preparing them for research and professional practice in computing.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CCS502

Course Title: Scientific Research Methods

Course Prerequisite: None

Course Description: This course is designed to equip master's students in computing with advanced knowledge to conduct rigorous, ethical, and impactful research in their field. This course covers the foundational principles of scientific research, including problem formulation, literature review, hypothesis and research question development, experimental design, data collection, analysis, simulation. By the end of the course, students will be prepared to undertake proposal research, contribute to scholarly publications, and address complex computing research challenges.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE501

Course Title: Cybersecurity Engineering

Course Prerequisite: None

Course Description: The Cybersecurity Engineering course provides master's students with advanced knowledge in cybersecurity domain. The curriculum covers core principles such as threat modelling, vulnerabilities exploitations and assessment, network security, intrusion detection/prevention systems alongside emerging topics like AI based IoT security, cloud security. Emphasis is placed on ethical hacking, digital forensics, social engineering. The case studies-based course prepares graduates to lead cybersecurity initiatives, safeguard critical infrastructure, and research solutions for evolving cyber threats.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE502

Course Title: Cybersecurity Models and Laws

Course Prerequisite: None

Course Description: This course explores key cybersecurity models such as Role-Based Access Control (RBAC), and Zero Trust Architecture (ZTA) alongside major frameworks such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001. It examines international and national legal frameworks including GDPR, the Budapest Convention, international and national cyber laws. Emphasis is placed on understanding the integration of technical models with regulatory requirements, enabling students to analyze and design secure systems that meet global compliance standards.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE503

Course Title: Game Theoretic Modeling

Course Prerequisite: None

Course Description: This course provides a rigorous introduction to game theory and its applications in computing, cybersecurity, economics, and strategic decision-making. Students will study fundamental concepts such as Nash equilibrium, dominant strategies, mixed strategies, repeated games, and cooperative vs. non-cooperative games. Emphasis is placed on applying these concepts to real-world scenarios including cybersecurity defence strategies, algorithmic decision-making, and competitive environments in digital systems. Students will develop the ability to formulate and solve complex strategic interaction problems.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE504

Course Title: Cybersecurity Governance and Risk Management

Course Prerequisite: None

Course Description: This course examines the principles, frameworks, and best practices essential for establishing effective cybersecurity governance and managing organizational risks that align organizational objectives with regulatory, technical, and ethical imperatives. Topics include governance structures, policy development, roles and responsibilities, risk assessment methodologies, and compliance with international standards. Students will learn how to align international cybersecurity models and initiatives with organizational objectives, evaluate organizational cybersecurity standing, evaluate threat landscapes, and implement risk mitigation strategies. Real-world case studies and regulatory contexts, such as GDPR and national cybersecurity laws are used to enhance strategic decision-making and policy formulation in enterprise environments.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE505

Course Title: Distributed Networks Security

Course Prerequisite: None

Course Description: This course focuses on the security challenges and solutions associated with distributed networks, including cloud infrastructures, blockchain-based networks, wireless sensor networks and IoT environments. Students will explore key concepts such as secure communication

protocols, distributed authentication, consensus mechanisms, intrusion detection, and fault tolerance in decentralized systems. Emphasis is placed on threat modeling, attack surfaces, and mitigation strategies in large-scale, heterogeneous networks.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE506

Course Title: Machine Learning for Cybersecurity

Course Prerequisite: None

Course Description: This course explores the application of machine learning techniques to detect, prevent, and respond to cybersecurity threats. Students will study supervised, unsupervised, and reinforcement learning approaches for tasks such as intrusion detection, malware classification, phishing detection, anomaly detection, and threat intelligence. The course emphasizes feature engineering, model evaluation, and handling adversarial attacks in cybersecurity contexts.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE507

Course Title: IoT applications and Security

Course Prerequisite: None

Course Description: This course examines the architecture, applications, and security challenges of the Internet of Things (IoT) in domains such as smart cities, smart homes, healthcare, transportation, and industrial systems. Students will explore IoT communication protocols, device integration, and data management alongside security concerns. Emphasis is placed on threat modeling, risk assessment, and applying security frameworks.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE601

Course Title: Secure Cloud Computing and Virtualization

Course Prerequisite: None

Course Description: Secure Cloud Computing and Virtualization explores the principles, architectures, and security challenges associated with cloud computing environments and virtualization technologies. The course examines cloud service models (IaaS, PaaS, SaaS), deployment models (public, private, hybrid), and the underlying virtualization techniques that enable scalable and efficient resource management. Emphasis is placed on security threats, data privacy, identity and access management, and compliance in virtualized and multi-tenant infrastructures. Students will analyze real-world case studies, evaluate cloud security frameworks, and apply best practices for securing cloud-based services and virtual environments.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE602

Course Title: Cyber Threats and Defense Strategies

Course Prerequisite: CSE501

Course Description: Cyber Threats and Defense Strategies provides an in-depth analysis of modern cyber threats, attack vectors, and the evolving tactics used by malicious actors. The course covers a wide range of threat landscapes, including malware, phishing, ransomware, advanced persistent threats and insider threats. Students will explore methods for threat detection, risk assessment, incident response, and the development of robust defense mechanisms using advanced frameworks. Through case studies and hands-on labs, learners will critically evaluate security architectures and implement proactive strategies to mitigate cyber risks across various organizational contexts.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE603

Course Title: Ethical Hacking and Penetration Testing

Course Prerequisite: CSE501

Course Description: Ethical Hacking and Penetration Testing offers a practical and theoretical foundation in cybersecurity techniques used to assess and strengthen information system defenses. The course guides students through the ethical and legal dimensions of hacking, emphasizing the responsibilities of a ethical hacker. Topics include reconnaissance, vulnerability analysis, exploitation, post-exploitation, and reporting.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE604

Course Title: Blockchain Technology and Cryptocurrency Security

Course Prerequisite: CSE501

Course Description: Blockchain Technology and Cryptocurrency Security explores the foundational principles, architecture, and security mechanisms of blockchain systems and digital currencies. The course examines distributed ledger technologies, consensus algorithms, smart contracts, and decentralized applications. Emphasis is placed on analyzing the security risks and vulnerabilities associated with blockchain platforms, wallet management, transaction privacy, and crypto-asset exchanges. Students will also study regulatory and ethical considerations, as well as techniques for securing blockchain infrastructures against emerging threats.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE605

Course Title: Secure Software Development and Code Analysis

Course Prerequisite: CSE501

Course Description: Secure Software Development and Code Analysis focuses on the integration of security throughout the software development lifecycle, emphasizing the design and implementation of robust, secure applications. The course covers secure coding practices, threat modeling, static and dynamic code analysis, risk assessment and mitigation of vulnerabilities. Students will learn to use industry tools for automated code scanning and vulnerability detection and will gain hands-on experience in identifying and fixing security flaws in real-world codebases. The course also addresses secure development standards and practices, and the role of compliance in modern software engineering.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE 606

Course Title: Advanced Cryptography and Security

Course Prerequisite: CSE501

Course Description: Advanced Cryptography and Security focuses on the theoretical foundations and practical applications of modern cryptographic techniques used to secure digital systems and communications. The course covers advanced topics related to public-key infrastructures, elliptic curve cryptography, zero-knowledge proofs, homomorphic encryption, and post-quantum cryptography. Students will examine cryptographic protocols that enable secure authentication, confidentiality, integrity, and non-repudiation in complex environments. Through case studies and hands-on exercises, learners will analyze real-world cryptographic implementations, evaluate emerging threats, and explore the role of cryptography in securing decentralized digital ecosystems.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE607

Course Title: Incident Response and Digital Forensics

Course Prerequisite: CSE501

Course Description: Incident Response and Digital Forensics provides a comprehensive understanding of strategies and methodologies used to detect, respond to, and investigate cybersecurity incidents. The course covers the incident response lifecycle, including preparation, detection, containment, eradication, recovery, and lessons learned. Students will learn about forensic tools and techniques for collecting, preserving, and analyzing digital evidence from compromised systems. Topics include malware analysis, chain of custody, legal and ethical considerations, and reporting procedures.

Credit Hours: 3

Weekly Contact Hours: 3

Course Code: CSE608

Course Title: Advanced Topics in Cybersecurity

Course Prerequisite: CSE501

Course Description: The course bridges cybersecurity principles and advanced threat mitigation strategies. The course explores recently published advanced and emerging cybersecurity methodologies, focusing on algorithmic and data-driven approaches to address complex, real-world security challenges. Topics may include, but are not limited to, adversarial machine learning, threat intelligence mining, secure system design, penetration testing, and cyber-physical system protection, with applications spanning

network security, digital forensics, and cloud environments. Emphasis is placed on analyzing recent research trends and translating them into practical, innovative defense strategies.

Credit Hours: 3

Weekly Contact Hours: 3