



**Ministry of Higher Education and Scientific Research
Scientific Supervision and Scientific
Evaluation Apparatus
Directorate of Quality Assurance and Academic
Accreditation
Accreditation Department**



Al-Huda University College

ACADEMIC PROGRAM DESCRIPTION

Department of Cyber Security Engineering Techniques

2026 - 2025

Introduction

An educational program is a coordinated and organized package of academic courses that includes procedures and learning experiences structured into course components. Its primary purpose is to develop and refine graduates' skills, enabling them to meet the requirements of the labor market. The program is reviewed and evaluated annually through internal or external quality assurance procedures, such as the External Examiner Program.

The Academic Program Description provides a brief summary of the main characteristics of the program and its courses, highlighting the skills that students are expected to acquire in accordance with the objectives of the academic program. This description is particularly important because it represents a fundamental basis for obtaining program accreditation. Faculty members contribute to its preparation under the supervision of the scientific committees within the academic departments.

In its second edition, this guide provides an updated description of the academic program following revisions to the components and sections of the previous guide, in light of the latest developments and changes in the Iraqi educational system. The guide includes the traditional forms of Academic Program Description based on the annual and semester systems, as well as the Academic Program Description adopted under the letter of the Department of Studies No. T M3/2906 dated 3 May 2023, concerning programs that adopt the Bologna Process as the basis for their academic structure and operation.

In this regard, we cannot overemphasize the importance of preparing accurate Academic Program and Course Descriptions to ensure the effective and efficient implementation of the educational process.

Concepts and Terminology

Academic Program Description:

The Academic Program Description provides a concise overview of the program's vision, mission, and objectives, including an accurate description of the intended learning outcomes in accordance with specified learning strategies.

Course Description:

The Course Description provides a concise overview of the main characteristics of the course and the expected learning outcomes that students are expected to achieve,

demonstrating whether they have fully benefited from the available learning opportunities. It is derived from the Academic Program Description.

Program Vision:

An aspirational image of the future of the academic program, reflecting its aim to become a developed, inspiring, motivating, realistic, and applicable program.

Program Mission:

A concise statement outlining the objectives and activities required to achieve them, while also identifying the program's development pathways and directions.

Program Objectives:

Statements describing what the academic program intends to achieve within a specified period of time. They should be measurable and observable.

Curriculum Structure:

All courses/subjects included in the academic program according to the adopted learning system (semester, annual, or Bologna Process), whether they are requirements of the Ministry, university, college, or academic department, together with the number of academic units.

Learning Outcomes:

A set of integrated knowledge, skills, and values acquired by students upon successful completion of the academic program. Learning outcomes should be specified for each course in a manner that contributes to achieving the objectives of the academic program.

Teaching and Learning Strategies:

The strategies used by faculty members to develop students' teaching and learning. They are plans and approaches followed to achieve learning objectives and describe all classroom and extracurricular activities designed to achieve the program's learning outcomes.

ACADEMIC PROGRAM DESCRIPTION FORM

College Name: Al-Huda University College

Scientific Department: Department of Cyber Security Engineering Techniques

Academic or Professional Program Name: Bachelor's Cyber Security Engineering Techniques

Final Certificate Name: Bachelor's Cyber Security Engineering Techniques

Academic System: Bologna

Description Preparation Date: 27/12/2025

File Completion Date: 27/12/2025

Signature

Head of Department

Dr. Mohammed Ayad Saad

Signature

Assistant Dean for Academic Affairs

Prof. Dr. Nadhim Abdullah Abd

Reviewed by

Quality Assurance and University Performance Unit

Name of QA Manager: MS.c. Mushtaq Mohammed Abdulnabi

Date: 2025/12/28

Signature:

Prof. Dr. Omar K.Mohammed Jasim

Dean

1. Program Vision

Al-Huda University College seeks to achieve excellence and leadership locally and across the Arab region, to raise the academic level through a commitment to academic rigour, and to be a leader in the field of higher education and scientific research.

2. Program Mission

To deliver high-quality academic programs that match scientific and technological developments locally and internationally, with the aim of preparing graduates capable of leadership and creativity in the scientific fields available at the college, and of serving society through effective participation in the various sectors of the state.

3. Program Objectives

1. To prepare and qualify an educated generation with high standards across the various sciences and fields of knowledge, capable of meeting the needs of the local and global labor market, admitting all students regardless of gender, sect or religion.
2. To prepare highly specialized cadres that make a difference in building Iraq, scientifically equipped to work with modern technologies and to keep pace with scientific development.
3. To strengthen scientific and cultural relations with local, Arab and international educational and scientific institutions in order to achieve the academic and developmental objectives of the college.
4. To provide advanced knowledge-based education that follows the latest developments while remaining committed to the authenticity of genuine Iraqi cultural heritage.
5. To contribute to the development of scientific research within Iraq and to keep pace with the scientific and cultural movement across the various fields of knowledge.
6. To raise the professional competence of academics, encourage them to conduct research and innovate, and promote electronic governance and information technology in the delivery of services.
7. To support specialized developmental and research projects and to translate knowledge into practical application in society.

4. Programmatic Accreditation

None

5. Other External Influences

None

6. Program Structure

Program Structure	Number of Courses	Study Units	Percentage	Notes
Institution Requirements	-	-	-	-
College Requirements	7	16 ECTS	6.66%	Supporting course
Department Requirements	41	224 ECTS	93.33%	Core + Elective (2 courses)
Summer Training	Available	Fulfilled	-	None
Other	-	-	-	-

7. Program Description

First Year | 2025 - 2026

Course Code	Course Name	Theoretical Hours	Practical Hours
CSTE1202	Ethics of the Information Age	2	0
CSTE1103	Programming Fundamentals	2	2
CSTE1102	Fundamentals of Electrical Engineering	2	2
CSTE1201	Digital Logic Design	2	2
HUC-1006	Democracy and Human Rights	2	0
EETC-102	Engineering Drawing	0	4
CSTE1104	Mathematics 1	3	0
CSTE1204	Mathematics 2	3	0
CSTE1203	General Physics	2	2
HUC-1002	English Language 1	2	0
HUC-1001	Arabic Language	2	0
EETC-101	Engineering Workshops	0	4
CSTE1101	Introduction to Information Systems	2	2

Second Year | 2026 - 2027

Course Code	Course Name	Theoretical Hours	Practical Hours
CSET2101	Engineering Mathematics	3	-
CSET2102	Fundamentals of Electronics	2	2
CSET2103	Principles of Linux	2	3
CSET2104	Computer Organization and Architecture	2	2
CSET2105	Data Structures and Algorithms	3	2
HUC1007	Crimes of the Ba'ath Regime in Iraq	2	-

Course Code	Course Name	Theoretical Hours	Practical Hours
CSET2201	Numerical Analysis and Statistics	2	-
CSET2202	Object-Oriented Programming	2	2
CSET2203	Microprocessors	3	2
CSET2204	Fundamentals of Communications	2	2
CSET2205	Introduction to Databases	3	2
HUC1003	English Language 2	1	-
HUC1009	Arabic Language 2	2	-

Third Year | 2027 - 2028

Course Code	Course Name	Theoretical Hours	Practical Hours
CSET3101	Computer Network Fundamentals	2	2
CSET3102	Information Security	2	2
CSET3103	Digital Signal Processing	2	2
CSET3104	Software Engineering	2	2
CSET3105	Python Programming	2	2
CSET31XX	Elective Course	2	2
CSET3201	Cybersecurity Fundamentals	2	2
CSET3202	Artificial Intelligence	2	2
CSET3203	Operating Systems	2	2
CSET3204	Web Design	2	3
CSET3205	Computer Network Protocols	2	2
CSET32XX	Elective Course	2	2

Fourth Year | 2028 - 2029

Course Code	Course Name	Theoretical Hours	Practical Hours
CSET4101	Advanced Cybersecurity	2	2
CSET4102	Network Security	2	3
CSET4103	Cloud Computing	2	2
CSET4104	Cybersecurity Governance	2	-
CSET4105	Project 1	-	-
CSET41XX	Elective Course	2	2
CSET4201	Ethical Hacking and Penetration Testing	2	2
CSET4202	Internet of Things Security	2	2
CSET4203	Mobile Phone Security	2	2
HUC1008	Professional Ethics	2	-
CSET4205	Project 2	-	-
CSET42XX	Elective Course	2	2

8. Expected Learning Outcomes of the Program

Knowledge

1. Comprehending the fundamental principles of cybersecurity and network systems, from the protection of data and systems through to incident response and risk management.
2. Understanding the design, implementation and operation of cyber systems and their associated control and security mechanisms.
3. The ability to operate, maintain and manage protection systems, firewalls and the software associated with digital infrastructure.
4. Analyzing complex technical and security problems using the principles of engineering, science and mathematics in order to find effective and secure solutions.
5. Designing experiments, penetration tests and measurement tests, and ensuring the security and quality of systems using contemporary engineering and technical tools.

Skills

1. Competence in carrying out practical operations and experiments within network and cybersecurity laboratories and engineering projects.
2. The ability to install, operate and test cyber protection systems and solutions, and to evaluate security performance and ensure its quality.
3. The ability to present technical security findings and reports orally and in writing, clearly and accurately, to managerial and technical audiences (such as risk-analysis and penetration-testing reports).
4. Skill in working within a multidisciplinary team and coordinating effectively in the implementation and securing of projects.

Values

1. Recognizing and adhering to the ethical and professional responsibilities associated with cybersecurity professional ethics (such as the protection of privacy and confidentiality) and their impact on society and the digital environment.
2. Applying safety and cybersecurity standards and quality assurance in engineering work environments and digital systems.
3. The ability to define objectives and work tasks, adhere to deadlines and manage cyber risks while working in varied environments.
4. Adapting to rapid changes and emerging threats in technology and to the requirements of the cybersecurity labor market.

9. Teaching and Learning Strategies

1. Interactive Theoretical Lectures

- Used to present and clarify the fundamental concepts, laws and theories in the fields of network security, cryptography, operating-system security and digital forensics.
- Instructors encourage students to ask questions, analyze ideas and take part in group discussion of contemporary cyber issues and threats.

2. Practical Laboratories

These enable students to translate theoretical knowledge into practical application, for example:

- Building and testing networked and secure environments.
- Using scanning tools and digital devices for packet analysis and penetration testing.
- Experimenting with protection solutions and configuring firewalls and access control.
- This strategy ensures learning grounded in experimentation and practical application.

3. Classroom Projects and Graduation Projects

- Motivate the student to use design and analysis skills to solve real security and cyber problems.
- Strengthen the capacity for research, innovation and teamwork.
- Examples: designing an intrusion detection system (IDS); building a secure environment for cryptography; building a system for monitoring and analyzing network vulnerabilities.

4. Problem-Based Learning

- Students are presented with a technical situation or a vulnerability / cyber attack on a network system and asked to analyze the problem and propose security solutions and protective measures.
- This develops skills of critical thinking, inference and decision-making in the management of digital crises.

5. Cooperative / Group Learning

- Students are asked to work in small teams on security projects, risk-analysis reports or presentations.
- This develops leadership and professional communication skills in a technical work environment.

6. Field Visits and Scientific Trips

- Students are taken to data centers, information-security companies and the communications and information-technology sectors.
- The aim is to link the academic side with practical reality and with the cybersecurity labor market.

10. Assessment Methods

1. Written Examinations (Midterm and Final)

- They include essay questions, computational / algorithmic questions and multiple-choice questions.

They are used to assess:

- Theoretical understanding of cybersecurity and network concepts.
- The ability to analyze and draw inferences about threats and vulnerabilities.
- The application of concepts in solving security and cryptographic problems.

2. Practical Assessment in the Laboratories

Based on the student's performance during the experiment in terms of:

- Understanding the steps for carrying out experiments and digital security procedures.
- The ability to use tools, software and network devices.
- Correctness of connections and of software and security configurations.
- Interpretation of results and analysis of vulnerabilities and event logs.
- The student usually submits a laboratory report which is assessed subsequently.

3. Project and Research Reports

These assess the student's ability to:

- Collect and analyze security information and data.
- Organize the report in a professional scientific and engineering style.
- Present proposed solutions or designs for secure protection systems.

4. Presentations and Oral Discussion

- Students are asked to present their projects or security research topics before the committee or their peers.

They are assessed on the basis of:

- Clarity of the idea and the security solutions proposed.
- The logical sequence of the presentation.
- Delivery skills and the defense of the work and the techniques used.

5. Assessment of Practical or Summer Training

Where summer training forms part of the program (in technology companies, data centers or information-security departments), assessment is based on:

- Professional and ethical adherence to working hours and workplace policies.
- The report of the training body and the development of practical skills in the field.
- The final report submitted by the student on the training period.

11. Faculty

Faculty Members

Academic Rank	General Specialization	Specific Specialization	Special Requirements / Skills (if any)	Staff	Lecturers
Lecturer	Chemical Engineering	Catalyst Technology	-	1	-
Lecturer	Electrical Engineering	Electronics	-	1	-
Assistant Lecturer	Electrical Engineering	Electrical Power	-	1	-
Assistant Lecturer	Computer Science	Artificial Intelligence	-	-	1

Professional Development - Induction of New Faculty Members

1. Ensuring that new faculty members are aligned with the vision, mission and objectives of the department and the college.
2. Supporting them in acquiring modern university teaching skills.
3. Developing their capabilities in scientific research, the use of technology and assessment methods.
4. Involving them in workshops on effective teaching methods, classroom management, interactive teaching and dealing with different student learning styles.
5. Training them in the use of e-learning systems and presentation and simulation tools.

Professional Development of Faculty Members

1. Improving the quality of teaching and learning methods.
2. Strengthening research capabilities and scientific publication.
3. Developing leadership and administrative skills.
4. Supporting integration between faculty members and the institution.
5. Keeping pace with technical and knowledge developments in the various specializations.
6. Integrating technology into education (blended learning and digital platforms).
7. Understanding local and international academic accreditation standards.

12. Admission Criteria

Admission channel for students graduating from preparatory schools, in its two branches:

1. Scientific branch, with an average of 59.5
2. Industrial branch, with an average of 61.5

13. Key Sources of Information About the Program

1. Fundamentals of Electric Circuits, C.K. Alexander and M.N.O. Sadiku, McGraw-Hill Education.
2. J. F. Wakerly, "Digital Design: Principles and Practices," 4th ed., Pearson Education, 2005.
3. K. A. Stroud and Dexter J. Booth, "Engineering Mathematics," 7th edition, Palgrave Macmillan, 2013.
4. J. Smith and E. Johnson, "Electrical Engineering Workshop: Theory and Practice."

14. Program Development Plan

1. Updating the curricula so that they keep pace with contemporary technological developments and cyber threats.
2. Strengthening the competence of faculty members and developing their skills in the latest digital security and protection techniques.
3. Linking the program to the labor market and to the requirements of development and of the technical and security sectors.
4. Developing the educational environment and the software and network laboratories (such as ethical hacking and digital forensics laboratories).
5. Moving towards institutional and programmatic academic accreditation.
6. Supporting applied scientific research in the fields of network security, cryptography, cloud computing and the security of technological systems.

Program Skills Map | First Year - 2025 / 2026

Course Code	Course Name	Core / Elective	Knowledge					Skills				Values			
			A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4
CSTE1202	Ethics of the Information Age	Core	✓	✓	✓			✓	✓			✓	✓		
CSTE1103	Programming Fundamentals	Core				✓				✓			✓		
CSTE1102	Fundamentals of Electrical Engineering	Core										✓			
CSTE1201	Digital Logic Design	Core				✓									
HUC-1006	Democracy and Human Rights	Core					✓			✓					✓
EETC-102	Engineering Drawing	Core										✓			
CSTE1104	Mathematics 1	Core				✓									
CSTE1204	Mathematics 2	Core										✓			
CSTE1203	General Physics	Core		✓											✓
HUC-1002	English Language 1	Core	✓	✓				✓					✓		
HUC-1001	Arabic Language	Core										✓			
EETC-101	Engineering Workshops	Core	✓	✓				✓	✓			✓	✓		
CSTE1101	Introduction to Information Systems	Core	✓	✓	✓			✓	✓			✓	✓		

Program Skills Map | Second Year - 2026 / 2027

Course Code	Course Name	Core / Elective	Knowledge					Skills				Values			
			A1	A2	A3	A4	A5	B1	B2	B3	B4	C1	C2	C3	C4
CSET2101	Engineering Mathematics	Core	✓	✓	✓			✓	✓			✓	✓		
CSET2102	Fundamentals of Electronics	Core				✓				✓			✓		
CSET2103	Principles of Linux	Core										✓			
CSET2104	Computer Organization and Architecture	Core				✓									
CSET2105	Data Structures and Algorithms	Core					✓			✓					✓
HUC1007	Crimes of the Ba'ath Regime in Iraq	Core										✓			
CSET2201	Numerical Analysis and Statistics	Core				✓									
CSET2202	Object-Oriented Programming	Core										✓			
CSET2203	Microprocessors	Core		✓											✓
CSET2204	Fundamentals of Communications	Core	✓	✓				✓					✓		
CSET2205	Introduction to Databases	Core													
HUC1003	English Language 2	Core										✓			
HUC1009	Arabic Language 2	Core										✓			

Program Skills Map | Third Year - 2027 / 2028

[illegible]

[illegible]