Republic of Iraq
Ministry of Higher Education & Scientific Research Supervision and Scientific Evaluation Directorate Quality Assurance and Academic Accreditation

Academic Program Specification Form for The Academic

University: Al-Zahrawi
COLLEGE SCIENCE
Department: Cybersecurity
Date Of Form Completion

313

prof. Dr. Hassan Jasim
Dean's Name

prof. Dr. Zainab M. Jawad
Dean's Assistant For Scientific Affairs

Head of Department
NAFSIN HASHIM

Date: 3/3/2026

Signature

Date: 3/3/2026

Signature

Date: / /

Signature

Quality Assurance And University Performance Manager Date: 3/3/2026
Signature

AL Zahraa Salman Ali

TEMPLATE FOR PROGRAMME SPECIFICATION

HIGHER EDUCATION PERFORMANCE REVIEW: PROGRAMME REVIEW

PROGRAMME SPECIFICATION

This Programme Specification provides a concise summary of the main features of the programme and the learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the learning opportunities that are provided. It is supported by a specification for each course that contributes to the programme.

1. Teaching Institution	Al-Zahrawi University
2. University Department/Centre	College of Science /Cybersecurity Department
3. Programme Title	Bachelor in Cybersecurity
4. Title of Final Award	Bachelor of Science (B.SC) in Cybersecurity
5. Modes of Attendance offered	Full-time / Morning study
6. Accreditation	Ministry of Higher Education and Scientific Research (MOHESR)
7. Other external influences	Market demands , IEEE/ACM Curricula , NIST Standards
8. Date of production/revision of this specification	March 2026
9. Aims of the Programme	
• Protecting Infrastructure: To provide students with deep knowledge of securing networks, cloud environments, and critical data systems.	
• Vulnerability Management: To enable students to identify, analyze, and mitigate cyber threats and system vulnerabilities.	
• Technical Proficiency: To develop advanced skills in cryptography, digital forensics, and secure software development.	
• Ethical & Legal Responsibility: To instill a strong sense of professional ethics and understanding of cyber laws and privacy regulations.	
• Adaptability: To prepare graduates for the rapidly evolving technological landscape by integrating AI-driven security and modern defense mechanisms.	

10. Learning Outcomes, Teaching, Learning and Assessment Methods

A. Knowledge and Understanding

A1. Understand the fundamental principles of computer science and information technology.

A2. Comprehend various cyber threats, attack vectors, and defense mechanisms.

A3. Knowledge of cryptography, data encryption, and information privacy standards.

A4. Familiarity with network protocols, cloud security, and hardware security.

A5. Understand legal, ethical, and professional issues in cybersecurity

A6. Knowledge of risk management and disaster recovery strategies.

B. Subject-specific skills

B1. Designing and implementing secure systems and network architectures.

B2. Conducting vulnerability assessments and penetration testing.

B3. Analyzing digital evidence and performing digital forensic investigations.

Teaching and Learning Methods

Lectures: Theoretical background and fundamental concepts.

- Practical Labs: Hands-on experience in cybersecurity tools and simulations.
- Group Projects: Developing teamwork and problem-solving skills.
- Case Studies: Analyzing real-world cyber-attack scenarios.

Assessment methods

- Written Exams: Midterm and final examinations to assess knowledge.
- Laboratory Reports: Evaluation of practical skills and findings.
- Quizzes: Frequent short tests to monitor student progress.
- Final Year Project: Assessing the ability to integrate and apply knowledge.

C. Thinking Skills

C1. Analytical Thinking: Ability to analyze complex cyber-attack scenarios and identify their root causes.

C2. Problem Solving: Developing innovative solutions to mitigate security risks and technical vulnerabilities.

C3. Critical Evaluation: Evaluating the effectiveness of different security protocols and tools.

C4. Logical Reasoning: Using logic to predict potential security threats and future system weaknesses.

Teaching and Learning Methods

• Interactive Workshops: Brainstorming sessions to solve cybersecurity challenges. • Scenario-based Learning: Simulating real-world security breaches. • Inquiry-based Learning: Encouraging students to research and find answers to complex technical questions.
Assessment methods
• Interactive Workshops: Brainstorming sessions to solve cybersecurity challenges. • Scenario-based Learning: Simulating real-world security breaches. • Inquiry-based Learning: Encouraging students to research and find answers to complex technical questions.

D. General and Transferable Skills (other skills relevant to employability and personal development)
D1. Communication Skills: Ability to explain technical security risks to non-technical stakeholders.
D2. Teamwork: Working effectively in groups to manage security incidents or develop projects.
D3. Time Management: Ability to prioritize tasks and meet deadlines in high-pressure environments.
D4. Lifelong Learning: Continuous self-development to keep up with the latest cyber threats and technologies.

Teaching and Learning Methods

Group Assignments: To enhance collaboration and leadership.
• Presentations: To develop public speaking and communication skills.
• Self-directed Learning: Researching new cybersecurity tools independently

Assessment Methods

• Peer Evaluation: Assessing contribution within a team.
• Oral Presentations: Evaluating communication and clarity.
• Project Documentation: Checking the quality of reports and technical writing.

11. Programme Structure				12. Awards and Credits
Level/Year	Course or Module Code	Course or Module Title	Credit rating	
first	ZU-SC-CS-1A-PF	Programming Fundamentals I	7	Bachelor Degree Requires (x) credits
first	ZU-SC-CS-1A-MC	Mathematics for Computing	4	
first	ZU-SC-CS-1A-CLE	Cybersecurity Laws and Ethics	4	
first	ZU-SC-CS-1A-CS	Computer Science Fundamentals	6	
first	ZU-SC-CS-1A-AR	Arabic	2	
first	ZU-SC-CS-1A-IC	Introduction to Cybersecurity	5	
first	ZU-SC-CS-1A-DHR	DEMECRACY AND HUMAN RIHTHTS	2	

12. Personal Development Planning

Encouraging students to obtain professional global certifications such as (CompTIA Security+, CEH, CISSP).
• Participating in Capture The Flag (CTF) competitions and cybersecurity hackathons to enhance practical skills.
• Organizing workshops and seminars on the latest cybersecurity trends and emerging cyber threats.
• Developing soft skills through student-led projects, presentations, and technical report writing.
• Providing career guidance and links to industry partners for internships and future employment.

13. Admission criteria .

• The applicant must hold a High School Diploma (Scientific Branch) or its equivalent.
• Admission is based on the minimum grade requirements set by the Ministry of Higher Education and Scientific Research for the current academic year.
• Students must pass any required placement tests or personal interviews conducted by the college (if applicable).
• Compliance with the general university admission regulations and medical fitness requirements.

14. Key sources of information about the programme

Official website of Al-Zahrawi University.
• The Ministry of Higher Education and Scientific Research (MOHESR) official portal and guidelines.
• College of Science student handbook and academic department brochures.
• Formal social media channels of the University and the Cybersecurity Department.
• The National Academic Reference Standards (NARS) for Computing and Information programs.

Curriculum Skills Map																			
please tick in the relevant boxes where individual Programme Learning Outcomes are being assessed																			
				Programme Learning Outcomes															
Year / Level	Course Code	Course Title	Core (C) Title or Option (O)	Knowledge and understanding				Subject-specific skills				Thinking Skills				General and Transferable Skills (or) Other skills relevant to employability and personal development			
				A1	A2	A3	A4	B1	B2	B3	B4	C1	C2	C3	C4	D1	D2	D3	D4
First	ZU-SC-CS-1A-IC	Introduction to Cybersecurity	C	*	*											*	*		
First	ZU-SC-CS-1A-AR	Arabic	O	*	*											*	*		
First	ZU-SC-CS-1A-CS	Computer Science Fundamentals	C	*	*											*	*		
First	ZU-SC-CS-1A-CLE	Cybersecurity Laws and Ethics	C	*	*											*	*		
First	ZU-SC-CS-1A-MC	Mathematics for Computing	C	*	*											*	*		
first	ZU-SC-CS-1A-PF	Programming Fundamentals I	C	*	*			*	*							*	*		
first	ZU-SC-CS-1A-DHR	Democracy and human		*	*											*	*		