Ministry of Higher Education and Scientific Research

Supervision and Scientific Evaluation Apparatus

Department of Quality Assurance and Academic Accreditation

International Accreditation Section

University of Babylon
College Of Information Technology
Dean Office

Academic Program Description

Academic Year: 2024 - 2025

University of Babylon
College Of Information Technology
Dean Office

University of Babylon

College of Information Technology

Cybersecurity Department

Number of Departments and Scientific Branches in the College: Three departments

Description Completion Date: 10/03/2025

Assoc. Prof. Dr. Ahmed Khelfa Al-Ajeli
Head of the Department
Date:12/3/ 2025

Prof. Dr. Iman Salih Sagban
Associate Dean for Academic Affairs
Date:12/3/ 2025

Prof. Dr. Wesam Sameer Bhaya
Dean of the College
Date:12/3 / 2025

Academic Program Description

This academic program description provides a concise summary of the key characteristics of the program and the expected learning outcomes that students should achieve, demonstrating whether they have maximized the available learning opportunities. It is accompanied by a description of each course within the program.

1. Institution	University of Babylon
2. College	Information Technology
3. Program Title	Cybersecurity
4. Degree	Bachelor of Science in Information Technology/Cybersecurity
5. Program Module	Semester-based
6. Accreditation	National Iraqi standards for Science degrees, based on Accreditation Board for Engineering and Technology (ABET).
7. Other external influencers	Surveys and joint workshops with industrial partners.
8. Date of completion/revision	10/03/2025

9. Program objectives

1. Educational Excellence
   - Deliver a curriculum that covers core principles of cyber security, including threat analysis, secure coding, digital forensics, and risk management.
   - Develop hands-on training and simulation environments for students to practice real-world cyber security skills.
   - Encourage ethical awareness and understanding of cyber security's social impact.
2. Research and Innovation
   - Conduct groundbreaking research on emerging threats, artificial intelligence in security and safe encryption methods.

- Collaborate with industry, government and academia to address current and future cyber threats.
- Publish findings and contribute to the body of knowledge in cyber security.

3. Community and Industry Engagement
   - Partner with local, national, and international organizations to improve cyber security best practices.
   - Organize workshops, seminars, and conferences to raise awareness and keep stakeholders informed on the latest cyber security trends.
4. Student Development and Career Advancement
   - Equip students with skills and certifications aligned with industry standards and demands.
   - Offer mentorship, internships, and career services to support student growth and transition into cyber security roles.

10. Learning Outcomes, and Teaching, Learning and Assessment Methods

A. Knowledge and understanding

A1. Understanding the fundamental principles of information security and risk management, including cyber threats, protection strategies, and cybersecurity-related regulations.

A2. Knowledge of network security, computer systems security, and advanced tools for detecting security vulnerabilities and potential weaknesses.

A3. Solutions and technologies for protecting data and digital infrastructure from various cyberattacks, including the use of encryption techniques, artificial intelligence, advanced authentication procedures, and application security to ensure data confidentiality, integrity, and availability.

A4. Digital forensic analysis methodologies for detecting and tracking suspicious activities, collecting digital evidence, and responding to cybersecurity incidents.

B- Practical skills

B1. Cybersecurity system analysis and design: The ability to analyze computing and network systems to identify security vulnerabilities and develop cybersecurity strategies and techniques, such as intrusion detection systems and encryption.

B2. Network, server, and website security: Involves implementing appropriate security protocols, access control, vulnerability management, and regularly updating systems to ensure protection against cyber threats.

B3. Digital forensic analysis: Utilizing cybersecurity forensic tools to collect and analyze digital evidence, identify the source of cyberattacks, and prepare necessary reports.

B4. Programming and software security: The ability to develop secure software using programming languages such as Python, C++, Java, and Flutter, and to detect security vulnerabilities in source code.

B5. Artificial intelligence in cybersecurity: Using AI tools to detect cyber threats and analyze big data to identify attack patterns.

Teaching and learning methods

1. Theoretical lectures
2. Project-based learning for solving real-world problems
3. Practical labs
4. Workshops and professional field training in cybersecurity
5. Self-directed and continuous learning

Assessment methods

1. Interactive assessment: This method ensures continuous interaction between students and content, enhancing learning quality through ongoing faculty feedback.

2. Theoretical exams: These exams assess students' understanding of fundamental cybersecurity concepts and their ability to analyze theoretical information.

3. Practical assessment: It evaluates students' capacity to apply security skills in realistic environments, preparing them for real-world professional challenges.

4. Individual and group projects: Students are tasked with applied projects that foster critical thinking, research, teamwork, and the practical application of theoretical knowledge.

5. Continuous assessment: Ongoing monitoring of student performance through assignments and activities ensures consistent academic development and skill improvement.

6. Reports and presentations: This assessment gauges students' ability to prepare and present technical reports on cybersecurity issues and solutions, enhancing

communication skills.

C. Critical-thinking Skills

C1. Enhancing critical and analytical thinking: This enables students to assess security threats and explore effective solutions.

C2. Fostering creativity and innovation: Encouraging students to find new and unconventional solutions to address cybersecurity challenges.

C3. Developing strategic thinking and long-term planning: This helps students create effective strategies to protect systems and information.

Teaching and learning methods

1. Cybersecurity competitions and challenges
2. Individual and group projects
3. Group brainstorming: Generating unconventional ideas to combat threats.
4. Case-based learning: Studying and analyzing previous cyberattacks.

Assessment methods

1. Performance-based assessment
2. Cybersecurity scenario tests
3. Practical exams and assessment using cybersecurity tools

D. Communication and Interpersonal Skills

D1. Collaboration and teamwork: The ability to work effectively within interdisciplinary teams, exchange knowledge, and contribute to solving security problems collectively.

D2. Task and time management: Effective planning and prioritization to complete tasks on time, with the ability to manage multiple projects simultaneously.

D3. Communication and leadership skills: The ability to express oneself clearly and professionally, both verbally and in writing, while enhancing leadership skills to manage teams and cybersecurity projects efficiently.

D4. Continuous learning and adaptability: A commitment to developing skills and staying updated on advancements in cybersecurity and artificial intelligence to adapt to rapid challenges and changes in the field.

Teaching and learning methods

1. Project-based learning for practical specialization subjects
2. Interactive workshops organized by the department staff and final-year students
3. Encouraging and motivating continuous self-directed learning

Assessment methods

1. Final project assessment to measure the quality and effectiveness of solutions
2. Practical assessment to monitor performance during implementation
3. Reports and surveys to measure progress, engagement, and benefit

11. Program Structure

Level	Course code	Name	ECTS credits 1 ECTS = 25 hours
I-1	CYSE1111	Introduction to Cybersecurity	5.00
	CYSE1112	Programming Fundamentals I	7.00
	CYSE1103	Computer Science Fundamentals	6.00
	CYSE1104	Cybersecurity Laws and Ethics	4.00
	CYSE1105	Mathematics for Computing	4.00
	CYSE1106	Arabic Language I	2.00
	CYSE1107	Democracy and Human Right	2.00
I-2	CYSE1201	Information Security Principles	5.00
	CYSE1202	Programming Fundamentals II	8.00
	CYSE1203	Computer Organisation and Architecture	6.00
	CYSE1204	Network Fundamentals	5.00
	CYSE1205	Probability and Statistics	4.00
	CYSE1206	English Language I	2.00

	II-1	CYSE2301	Object-Oriented Programming	6.00
		CYSE2312	Web Design	6.00
		CYSE2313	Information Theory and Coding	4.00
		CYSE2304	Internet Architecture	6.00
		CYSE2315	Database Systems	6.00
		CYSE2306	English Language II	2.00
	II-2	CYSE2401	Malicious Software	4.00
		CYSE2402	Data Structures and Algorithms	6.00
		CYSE2413	Web Application Development	6.00
		CYSE2404	Cryptography	6.00
		CYSE2415	Software Security Principles	4.00
		CYSE2406	Arabic Language II	2.00
		CYSE2407	Crimes of the Baath Regime in Iraq	2.00
	III-1	CYSE3511	Artificial Intelligence	5.00
		CYSE3502	Web Security	5.00
		CYSE3503	Incident Response Management	5.00
		CYSE3514	Operating Systems	5.00
		CYSE3505	Software Development and Security	5.00
		CYSE3516	Mobile Programming	5.00
	III-2	CYSE3601	Machine Learning	6.00
		CYSE3602	Network Security	6.00
		CYSE3603	Database Systems Security	5.00

		CYSE3604	Cyber Threat Intelligence	5.00
		CYSE3605	Operating Systems Security	6.00
		CYSE3606	Social Engineering	2.00
	IV-1	CYSE4701	Ethical Hacking	7.00
		CYSE4702	Server Administration	6.00
		CYSE4703	Social Networks Security	3.00
		CYSE4704	Access Control	6.00
		CYSE4705	Systems 'Monitoring	4.00
		CYSE4716	Project I	4.00
	IV-2	CYSE4801	Mobile Application Security	6.00
		CYSE4802	Cloud Computing	4.00
		CYSE4803	Digital Forensics	5.00
		CYSE4804	Introduction to Multimedia Security	5.00
		CYSE4805	Hardware Security	6.00
		CYSE4806	Project II	4.00

12. Degree requirements

Bachelor degree requires (240) ECTS credits and summer internship. Each ECTS unit is equivalent to 25 structured and unstructured hours.

13. Personal Development Planning

1. Acquiring skills in programming fundamentals, encryption, and cybersecurity.
2. Developing the ability to conduct research and formal job interviews.
3. Gaining skills in IT fundamentals, collaboration, and fostering teamwork spirit.

14.Admission criteria

For Iraqi students, the student guide for centralized admission to public universities, issued by the Ministry of Higher Education and Scientific Research, is here.
For international students, the university and ministry instructions within the "Study in Iraq" program are followed.
The instructions links: https://www.uobabylon.edu.iq/main/international.aspx and https://studyiniraq.scrd-gate.gov.iq/home.

15.Key information sources about the program

The department website:
https://it.uobabylon.edu.iq/department/Default.aspx?cdid=3

Curriculum Skills Table 1

Year/ Level	Course Code	Name	Type	Learning Outcomes															
				A. Knowledge and understanding				B- Practical skills					C. Critical-thinking Skills			D. Communication and Interpersonal Skills			
				A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	C2	C3	D1	D2	D3	D4
First year/ Autumn	CYSE1111	Introduction to Cybersecurity	Core	✔	✔			✔	✔	✔		✔	✔		✔	✔	✔	✔	✔
	CYSE1112	Programming Fundamentals I	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1103	Computer Science Fundamentals	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1104	Cybersecurity Laws and Ethics	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1105	Mathematics for Computing	Support	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1106	Arabic Language I	Basic												✔	✔	✔	✔	✔
	CYSE1107	Democracy and Human Right	Basic												✔	✔	✔	✔	✔
First year/ Spring	CYSE1201	Information Security Principles	Core	✔	✔	✔		✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1202	Programming Fundamentals II	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1203	Computer Organisation and Architecture	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1204	Network Fundamentals	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1205	Probability and Statistics	Support		✔	✔					✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE1206	English Language I	Basic										✔	✔	✔	✔	✔	✔	✔

Curriculum Skills Table 2

Year/ Level	Course Code	Name	Type	Learning Outcomes															
				A. Knowledge and understanding				B- Practical skills					C. Critical-thinking Skills			D. Communication and Interpersonal Skills			
				A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	C2	C3	D1	D2	D3	D4
Second year/ Autumn	CYSE2301	Object-Oriented Programming	Core	✔	✔	✔		✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE2312	Web Design	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE2313	Information Theory and Coding	Support	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE2304	Internet Architecture	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE2315	Database Systems	Core	✔		✔		✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE2306	English Language II	Support					✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
Second year/ Spring	CYSE2401	Malicious Software	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE2402	Data Structures and Algorithms	Core	✔	✔				✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE2413	Web Application Development	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE2404	Cryptography	Core	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE2415	Software Security Principles	Core	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE2406	Arabic Language II	Basic										✔	✔	✔	✔	✔	✔	✔
	CYSE2407	Crimes of the Baath Regime in Iraq	Basic										✔		✔	✔		✔	

Curriculum Skills Table 3																			
Year/ Level	Course Code	Name	Type	Learning Outcomes															
				A. Knowledge and understanding				B- Practical skills					C. Critical-thinking Skills			D. Communication and Interpersonal Skills			
				A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	C2	C3	D1	D2	D3	D4
Third year/ Autumn	CYSE3511	Artificial Intelligence	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3502	Web Security	Core			✔	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔
	CYSE3503	Incident Response Management	Core	✔			✔	✔		✔			✔	✔	✔	✔	✔	✔	✔
	CYSE3514	Operating Systems	Core	✔	✔				✔	✔	✔		✔		✔	✔	✔	✔	✔
	CYSE3505	Software Development and Security	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3516	Mobile Programming	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Third year/ Spring	CYSE3601	Machine Learning	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3602	Network Security	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3603	Database Systems Security	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3604	Cyber Threat Intelligence	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3605	Operating Systems Security	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE3606	Social Engineering	Core	✔	✔			✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Curriculum Skills Table 4

Year/ Level	Course Code	Name	Type	Learning Outcomes															
				A. Knowledge and understanding				B- Practical skills					C. Critical-thinking Skills			D. Communication and Interpersonal Skills			
				A1	A2	A3	A4	B1	B2	B3	B4	B5	C1	C2	C3	D1	D2	D3	D4
Fourth year/ Autumn	CYSE4701	Ethical Hacking	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4702	Server Administration	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4703	Social Networks Security	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4704	Access Control	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4705	Systems 'Monitoring	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4716	Project I	Core	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔
Fourth year/ Spring	CYSE4801	Mobile Application Security	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4802	Cloud Computing	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4803	Digital Forensics	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4804	Introduction to Multimedia Security	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4805	Hardware Security	Core	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CYSE4806	Project II	Core	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔