

University of Warith Al-Anbiyaa

جامعة وارث الانبياء



First Cycle – Four Levels – 240 ECTS
Bachelor's Degree (B.Sc.) - Cybersecurity

الدورة الأولى - بكالوريوس علوم الامن السيبراني - أربع سنوات - ٢٤٠ وحدة اوربية



م.د. محمد علي الغانم
العميد
٢٠٢٣ - ٢٠٢٥



م.د. علي كريم عبد الرحمن
ر.ق. ١٨٣٣ السيبراني
٢٠٢٣ - ٢٠٢٥

Table of Contents | جدول المحتويات

1. Vision & Mission Statement	بيان الرؤية والرسالة
2. Program Goals	أهداف البرنامج
3. Program Specification Overview	مواصفات البرنامج
4. Program learning outcomes	مخرجات تعلم الطالب على مستوى البرنامج الدراسي
5. Academic Staff	الهيئة التدريسية
6. Credits, Grading and GPA	الاعتمادات والدرجات والمعدل التراكمي
7. Modules	المواد الدراسية
8. Contact	اتصال

1. Vision & Mission Statement

Vision Statement

To be a distinguished Cybersecurity program in Iraq and the region, recognized for academic excellence, innovative research, and producing highly qualified graduates capable of protecting digital infrastructures, enhancing information security, and contributing to national digital transformation and sustainable technological development.

Mission Statement

The Cybersecurity Department is committed to:

- Providing high-quality undergraduate education in cybersecurity that complies with international academic standards and the Bologna Process framework.
- Developing students' analytical thinking, technical skills, and ethical professional practices through modern teaching methodologies, virtual labs, and hands-on security environments.
- Serving the community and public sector through cyber awareness initiatives, risk assessment, and evidence-based cybersecurity solutions.
- Preparing graduates with the knowledge and professional skills required for careers in cybersecurity operations, information assurance, security governance, and related ICT fields.

2. Program Goals

- Ensure graduates master fundamental and advanced cybersecurity concepts in alignment with Iraqi higher education standards and international best practices.

- Develop students' practical and research capabilities through modern laboratories, cybersecurity simulations, and industry-oriented projects.
- Promote understanding of cyber threats, risk management, and the protection of national digital assets and critical infrastructures.
- Contribute to sustainable digital development by supporting secure information systems, innovation, and responsible use of emerging technologies

3. Program Specification Overview

Programme code:	BSc-CyS	ECTS	240
Duration:	4 levels, 8 Semesters	Method of Attendance:	Full Time

The Bachelor of Science in Cybersecurity is a four-year undergraduate program designed in full compliance with the Bologna Process framework, comprising 240 ECTS credits distributed across eight semesters. The program adopts the European Credit Transfer and Accumulation System (ECTS), where one ECTS corresponds to 25 hours of student workload, including lectures, practical laboratories, independent study, projects, and assessment activities.

Level 1 exposes students to the fundamentals of computer, and computer security suitable for progression to all programs within the computer program group. Program-specific core topics are covered at Level 2 preparing for research-led subject specialist modules at Levels 3 and 4. A computer science graduate is therefore trained to appreciate how research informs teaching, according to the University and School Mission statements. At Levels 2, 3 and 4 students are more than half of their specialist in the field of computer and cyber security modules. This allows students to develop their own wide-ranging interests in computer field. Decisions on what to study are made with input from personal tutors.

The curriculum is structured to provide students with a strong and progressive foundation in cybersecurity and information technology, beginning in the first year with fundamental courses in computer science, programming, mathematics, discrete structures, networking basics, and operating systems. In subsequent years, the program advances to specialized cybersecurity disciplines such as network security, cryptography, secure systems design, ethical hacking, digital forensics, malware analysis, cloud and IoT security, risk management, and cybersecurity governance.

The program allocates approximately 50% of the total credits to core cybersecurity modules, 20% to supporting and elective modules that enable students to develop specialized technical or managerial competencies, and places strong emphasis on practical and applied learning, with 30% of credits dedicated to laboratory work, hands-on security exercises, simulation-based training, case studies, industry-oriented projects, and professional internships.

4. Program Learning Outcomes

4.1 Knowledge and Understanding (K)

- K1.** Demonstrate comprehensive knowledge of core cybersecurity concepts, including information security principles, threat landscapes, and defense mechanisms.
- K2.** Explain the fundamentals of computer networks, operating systems, cryptography, and secure software systems.
- K3.** Describe common cyber threats, vulnerabilities, attack vectors, and security controls across digital systems.
- K4.** Understand cybersecurity policies, standards, legal frameworks, and ethical considerations at national and international levels.

4.2 Intellectual/Cognitive Skills (C)

- C1.** Analyze cybersecurity problems and assess risks using systematic and analytical approaches.
- C2.** Evaluate security incidents, vulnerabilities, and attack scenarios to propose appropriate mitigation strategies.
- C3.** Apply critical thinking to interpret technical reports, security logs, and threat intelligence data.
- C4.** Design secure solutions and make evidence-based decisions in complex cybersecurity contexts.

4.3 Practical and Professional Skills (P)

- P1.** Use cybersecurity tools and technologies for network security, system hardening, and vulnerability assessment.
- P2.** Perform practical security tasks such as penetration testing, digital forensics, and incident response in controlled environments.
- P3.** Configure and manage secure networks, operating systems, and applications following best practices.
- P4.** Apply professional standards, ethical guidelines, and safety procedures in cybersecurity operations.

4.4 General and Transferable Skills (T)

- T1.** Communicate cybersecurity concepts, risks, and solutions effectively in written and oral forms.
- T2.** Work effectively as an individual and as a member of multidisciplinary teams.
- T3.** Use information technology, security software, and analytical tools efficiently for learning and problem-solving.
- T4.** Demonstrate self-directed learning, adaptability, and continuous professional development in the cybersecurity field.

5. Academic Staff

Ali Kareem Abdul Raheem | Ph.D. in Information Technology – Artificial Intelligence.

Email: alialmujab@uowa.edu.iq

Mobile no.:07725106635

Radwan Jawad Kazem | Ph.D. in Computer Security and Cyber Security.

Email: Radhwanjawadkadhim@gmail.com

Mobile no.: 07735316612

Maky H.Abdulraheem | Ph.D. in Computer Science.

Email: maky.h@uowa.edu.iq

Mobile no.: 7711889739

Nabil Sadiq Abdul abbas | M.Sc. in Computer Science.

Email: nabeel@uowa.edu.iq

Mobile no.: 7733125323

Elaf Ali Safooq | M.Sc. in Computer Science and Mathematics.

Email: elaf.safooq@uowa.edu.iq

Mobile no.: 7722291607

6. Credits, Grading and GPA

Credits

University of Warith Al-Anbiyaa is following the Bologna Process with the European Credit Transfer System (ECTS) credit system. The total degree program number of ECTS is 240, 30 ECTS per semester. 1 ECTS is equivalent to 25 hrs student workload, including structured and unstructured workload.

Grading

Before the evaluation, the results are divided into two subgroups: pass and fail. Therefore, the results are independent of the students who failed a course. The grading system is defined as follows:

GRADING SCHEME مخطط الدرجات				
Group	Grade	التقدير	Marks (%)	Definition
Success Group	A - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors

(50 - 100)	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 - 49)	FX – Fail	راسب - قيد المعالجة	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note:				

Note: Marks with Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.

ملاحظة: سيتم تقرير العلامات العشرية التي تزيد أو تقل عن .5 إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، سيتم تقرير علامة ٥٤.٥ إلى ٥٥، بينما سيتم تقرير علامة ٥٤.٤ إلى ٥٤). لدى الجامعة سياسة لا تسمح بـ "حالات الرسوب القريبة من النجاح"، لذا فإن التعديل الوحيد للعلامات الممنوحة من قبل المصححين الأصليين سيكون التقرير التلقائي الموضح أعلاه.

Calculation of the Cumulative Grade Point Average (CGPA)

1. The CGPA is calculated by the summation of each module score multiplied by its ECTS, all are divided by the program total ECTS.

CGPA of a 4-year B.Sc. degree:

$$\text{CGPA} = [(1\text{st module score} \times \text{module ECTS}) + (2\text{nd module score} \times \text{module ECTS}) + (3\text{rd module score} \times \text{module ECTS}) + \dots + (\text{last module score} \times \text{module ECTS})] / 240$$

7. Curriculum/Modules

Semester 1 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
Cys1101	Data Security Principles	48	77	5.00	C	
CSIT1102	Calculus I	48	77	5.00	B	
CYS1103	Programming Fundamentals I	78	97	7.00	C	
CSIT1104	Digital Logic	78	72	6.00	B	
Cys1105	Computer Organization	63	62	5.00	C	
UOWA103	Arabic Language I	33	17	2.00	S	

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
Cys1201	Cybersecurity Principles	48	152	8.00	C	

CSIT1212	Calculus II	48	77	5.00	B	CSIT501
Cys1213	Discrete Structure	48	102	6.00	B	
Cys1204	Programming Fundamentals II	78	97	7.00	C	Cys102
UOWA101	English Language I	33	17	2.00	S	
UOWA102	Human Rights and Democracy	33	17	2.00	S	

8. **Contact**

Program Manager:

Ali Kareem Abdul Raheem | Ph.D. in Information Technology - Artificial Intelligence.

Email: alialmujab@uowa.edu.iq

Mobile no.:07725106635