

University of Mosul

جامعة الموصل



First Cycle – Four Levels – 240 ECTS

Bachelor's Degree (B.Sc.) - Cyber Security

الدورة الأولى - بكالوريوس علوم في الأمن السيبراني - أربع سنوات - ٢٤٠ وحدة ائتمانية
كلية علوم الحاسوب والرياضيات | قسم الأمن السيبراني



Table of Contents | جدول المحتويات

1. Vision & Mission Statement
2. Program Goals
3. Program Specification Overview
4. Program learning outcomes
5. Academic Staff
6. Credits, Grading and GPA
7. Modules
8. Contact

1. Vision & Mission Statement

Vision Statement

Excellence and leadership in the educational, professional and research field of cybersecurity at the regional and global levels. And commitment to effectively meet the needs of society and the labor market.

Mission Statement

Preparing professional cadres in cybersecurity in both the academic and professional fields capable of leading, designing and developing various projects in the various fields of cybersecurity, by providing a distinguished and high-quality program that focuses on integrating scientific theories and practical training to develop programs and applications and innovation in scientific research and provide the required security services to individuals and public and private institutions in Iraq and contribute to the development of society.

2. Program Goals

- 1- Providing students with the knowledge, skills and behaviors necessary to analyze cybersecurity problems and design appropriate solutions through best practices to enable them to excel and innovate and qualify them for the best positions in the labor market.
- 2- The ability to innovate while adhering to the professional, legal and ethical framework and working effectively within multidisciplinary work teams.
- 3- Enabling the student to engage in continuous self-learning to continue enhancing their skills and learn about the latest developments in the cybersecurity technology industry and adopt new technologies and methods.
- 4- The ability to enroll in graduate programs in cybersecurity topics and other topics.

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 Cyber Security at the University of Mosul, delivered by the College of Computer Science and Mathematics, is a four-year full-time undergraduate program designed in full compliance with the Bologna Process framework, comprising 240 ECTS credits distributed across eight semesters. The program follows the European Credit Transfer and Accumulation System (ECTS), where one ECTS equals 25 hours of student workload, encompassing lectures, laboratory sessions, security exercises, self-study and assessment activities. The specialization was established in response to the rapid pace of digital transformation and the resulting rise in cyber attacks and system-intrusion risks, and after consultation with specialists in computer science and with the public and private labour market, in order to prepare national expertise capable of strengthening the cyber security infrastructure of Iraq and improving the performance and safety of public and private institutions. The curriculum combines a solid foundation in programming, computer science, mathematics and networking with specialized study of information security, cryptography, ethical hacking, digital forensics, cyber warfare, cloud computing, and the security of networks, databases, web applications and the Internet of Things. Programming and scripting languages relevant to cyber security and cloud computing, notably Python, are embedded across the stages of the curriculum for the development of security tools. Theoretical knowledge is integrated with laboratory work, hands-on security exercises, project-based learning and a two-part graduation research project, so that graduates acquire the analytical, practical and problem-solving capabilities required to protect information systems, networks, applications and digital infrastructure, while the program also fosters ethical responsibility, teamwork, innovation and continuous professional development.

Qualification Awarded

On successful completion of the program requirements, the graduate is awarded the degree of Bachelor of Science (B.Sc.) in Cyber Security from the University of Mosul.

Level of Qualification

The program is classified at Level 6 of the Iraqi National Qualifications Framework (INQF), or its equivalent, in accordance with the regulations and directives of the Ministry of Higher Education and Scientific Research.

Specific Admission Requirements

Admission to the B.Sc. in Cyber Security is governed by the admission regulations and policies of the Ministry of Higher Education and Scientific Research and the University of Mosul. Applicants must satisfy the approved central admission criteria for the College of Computer Science and Mathematics.

Recognition of Prior Learning (RPL)

Recognition of prior learning and credit transfer are considered only in cases of student transfer or module equivalence, in accordance with the regulations and instructions of the Ministry of Higher Education and Scientific Research and the University of Mosul.

Requirements for the Award of the Qualification

- Completion of all 240 ECTS credits across eight semesters (four years), including all compulsory modules specified in the curriculum.
- Achievement of the minimum graduation requirements, including the required GPA, in accordance with the regulations of the Ministry of Higher Education and Scientific Research and the University of Mosul.
- Successful completion of the graduation research project (Project 1 and Project 2) and of all required laboratory work, security-tool training and other practical components of the program.
- Completion of a summer internship of not less than four weeks, as required for the award of the Bachelor's degree.
- Compliance with all academic regulations governing assessment, academic progression and graduation, and satisfaction of all academic and administrative requirements for the award of the degree.

Mode of Study

The B.Sc. in Cyber Security is a full-time, four-year undergraduate program delivered in accordance with the Bologna Process and comprising 240 ECTS credits across eight semesters. It adopts a student-centred approach that integrates theoretical lectures, laboratory work, hands-on security exercises, project-based learning and a two-part graduation project. These activities are supported by seminars, technical workshops and a four-week summer internship intended to strengthen students' technical competence, digital skills and readiness for professional practice.

Examination, Assessment and Grading

The program applies the examination, assessment and grading regulations approved by the Ministry of Higher Education and Scientific Research and the University of Mosul. Student performance is assessed through a range of formative and summative methods, including continuous assessment (quizzes, assignments and classroom activities), midterm examinations, final examinations, laboratory reports and practical assessments, security-tool exercises and practical work, the summer internship of not less than four weeks, oral presentations and seminars, and assessment of the graduation project (Project 1 and Project 2), together with compliance with academic integrity regulations and institutional policies on academic misconduct, cheating and plagiarism.

Graduate Career Profiles

Graduates of the B.Sc. in Cyber Security are qualified for a wide range of roles in the public and private sectors, including:

- Information Security Analyst / Information Security Manager.
- Network Security Engineer / Network Security Administrator.
- Penetration Tester and Ethical Hacker.

- Digital Forensics Analyst / Cybercrime Investigator.
- Security Operations Centre (SOC) Analyst and First Incident Responder.
- Cloud Security Architect.
- Application and Web Application Security Officer.
- Data Privacy Officer and Governance, Risk and Compliance (GRC) Manager.
- Cryptographer and Public Key Infrastructure (PKI) Analyst.
- IoT and Industrial Control Systems (SCADA) Security Specialist.
- Chief Information Security Officer (CISO) and other leadership roles in public and private institutions, banks, oil and gas companies and government bodies requiring cyber security expertise.

4. Program Learning Outcomes

4.1 Knowledge and Understanding (K)

- K1.** Demonstrate a comprehensive understanding of computing fundamentals, programming, mathematics and computer networks as the basis of cyber security practice.
- K2.** Explain the core principles of information security, including confidentiality, integrity, availability, authentication and non-repudiation.
- K3.** Describe cryptographic concepts, algorithms and key-management mechanisms and their role in securing data and communications.
- K4.** Explain the architecture, protocols and vulnerabilities of computer networks, operating systems, databases and web applications.
- K5.** Identify the categories of cyber threats and attacks, including malicious code, intrusion techniques and cyber-warfare methods.
- K6.** Describe the principles of digital forensics and incident response and the requirements for sound digital evidence.
- K7.** Explain the security requirements of cloud computing and Internet of Things environments.
- K8.** Understand information risk management, data privacy, and the legal, ethical and professional framework governing cyber security practice in Iraq.

4.2 Intellectual/Cognitive Skills (C)

- C1.** Identify, formulate and analyse cyber security problems by applying the principles of computer science, mathematics and information security.
- C2.** Analyse systems, networks and applications in order to discover vulnerabilities and assess their severity and impact.
- C3.** Design secure systems, networks, applications, cloud environments and Internet of Things environments that meet defined security requirements.
- C4.** Evaluate security tools, controls and countermeasures and select those appropriate to a given context.
- C5.** Interpret the output of security tools, logs and forensic artefacts in order to reach evidence-based conclusions.

- C6.** Apply risk-management and threat-modelling methods to prioritise protective measures.
- C7.** Evaluate scientific literature, standards and best practice in cyber security critically.
- C8.** Exercise sound professional judgement that takes account of societal, legal and institutional consequences.

4.3 Practical and Professional Skills (P)

- P1.** Use cyber security tools and techniques competently, including penetration testing, digital forensics and malicious-code analysis.
- P2.** Implement and configure security controls for networks, operating systems, databases and web applications.
- P3.** Write programs and scripts, including in Python, to build and automate security tools.
- P4.** Conduct ethical hacking and vulnerability-assessment exercises within a lawful and authorised framework.
- P5.** Perform digital forensic acquisition and analysis and preserve the chain of custody of evidence.
- P6.** Apply cryptographic mechanisms and secure communication protocols in practice.
- P7.** Secure cloud computing and Internet of Things deployments.
- P8.** Detect, respond to and document security incidents and produce clear technical reports and documentation.

4.4 General and Transferable Skills (T)

- T1.** Communicate cyber security matters effectively to technical and non-technical audiences in both English and Arabic.
- T2.** Work effectively within multidisciplinary teams and lead group work.
- T3.** Plan and manage security tasks, adhere to deadlines and manage risk.
- T4.** Use information technology, professional software and technical documentation effectively.
- T5.** Present findings through seminars, oral presentations and written reports.
- T6.** Search for, evaluate and use scientific literature and technical sources.
- T7.** Demonstrate self-directed learning and continuous professional development as the field evolves.
- T8.** Demonstrate ethical, legal and professional responsibility and serve the community responsibly.

4.5 Alignment with Graduate Outcomes (GOs) and the Iraqi National Qualifications Framework (INQF – Level 6)

The program learning outcomes above are aligned with the seven Graduate Outcomes (GOs) adopted by the Department of Cyber Security and with the key learning domains of the Iraqi National Qualifications Framework at Level 6, as follows:

- Knowledge and Understanding (K1–K8) — GO1, GO2 — INQF domain: Knowledge and Understanding: comprehensive knowledge of computing fundamentals, information security principles, cryptography and network security, used to identify, analyse and address cyber security problems in line with recognised standards and practice.

- Intellectual and Cognitive Skills (C1–C8) — GO1, GO2, GO5 — INQF domain: Skills: application of cyber security tools and techniques, including penetration testing, digital forensics, malicious-code analysis and security auditing, to detect and respond to vulnerabilities and intrusions and to reach sound engineering decisions.
- Practical and Professional Skills (P1–P8) — GO2, GO3 — INQF domain: Application: design, implementation and evaluation of secure systems, applications, networks, cloud environments and Internet of Things environments, applying risk management principles and engineering quality standards to protect public, private and governmental infrastructure.
- General and Transferable Skills (T1–T8) — GO4, GO5, GO6, GO7 — INQF domain: Values: effective communication, teamwork, ethical and professional responsibility, leadership, and commitment to lifelong learning and professional development in the service of society.

5. Academic Staff

Oday Hashim Saeed Al-Wattar (Head of Department) | Ph.D. | Assistant Prof.

Email: ahsa.alwattar@uomosul.edu.iq

Mobile no.:

Faris Adel Hamed | Ph.D. | Assistant Prof.

Email: f.lwaaah@uomosul.edu.iq

Mobile no.:

Ann Akram Jarjees Al-Qazzaz | Ph.D. | Lecturer

Email: annkazzaz@uomosul.edu.iq

Mobile no.:

Ahmed Sami Nuri Al-Qutchi | Ph.D. | Assistant Prof.

Email: ahmed.s.nori@uomosul.edu.iq

Mobile no.:

Asmaa Mohammed Sulaiman Hussein Al-Ali | M.Sc. | Assistant Lecturer

Email: asmaa.mohammed.s@uomosul.edu.iq

Mobile no.:

Ibrahim Mohammed Ahmed | Ph.D. | Assistant Prof.

Email: ibrahim_alhlma@uomosul.edu.iq

Mobile no.:

Ziyad Safaa Younis Sfawi | Ph.D. | Lecturer

Email: zeyad.saffawi@uomosul.edu.iq

Mobile no.:

Karam Hatem Thanoon | Ph.D. | Assistant Prof.

Email: Karamhatim@uomosul.edu.iq

Mobile no.:

Rahma Nizar Ibrahim | M.Sc. | Assistant Lecturer

Email: rahma.nazar@uomosul.edu.iq

Mobile no.:

Sura Sabah Ibrahim Ahmed Al-Sharifi | M.Sc. | Assistant Lecturer

Email: sura.s@uomosul.edu.iq

Mobile no.:

Sufyan Salim Mahmood Al-Dabbagh | Ph.D. | Assistant Prof.

Email: drsufyan.salim@uomosul.edu.iq

Mobile no.:

Sundus Abdul-Muttalib Mohammed | M.Sc. | Lecturer

Email: sundus_abid7@uomosul.edu.iq

Mobile no.:

Shaimaa Fahad Rashid | M.Sc. | Assistant Lecturer

Email: Shaimaa.fahad@uomosul.edu.iq

Mobile no.:

Omar Abd Najm Al-Nuaimi | M.Sc. | Assistant Lecturer

Email: omar.a.n@uomosul.edu.iq

Mobile no.:

Muna Khalaf Omar Owaid Al-Saawi | M.Sc. | Assistant Lecturer

Email: muna.khalaf@uomosul.edu.iq

Mobile no.:

Nadia Maan Mohammed Thabit | Ph.D. | Assistant Prof.

Email: nadia.m.mohammed@uomosul.edu.iq

Mobile no.:

Nihad Hasan | M.Sc. | Assistant Lecturer

Email: nehad.hussein@uomosul.edu.iq

Mobile no.:

Wedyan Safaa Mahmood Ali Al-Nuaimi | M.Sc. | Assistant Lecturer

Email: wdean.safa@uomosul.edu.iq

Mobile no.:

Shaimaa Shakeeb | Ph.D. | Lecturer

Email: shymsak@uomosul.edu.iq

Mobile no.:

Omar Haitham Mohammed | Ph.D. | Lecturer

Email: omar.alhabeeb@uomosul.edu.iq

Mobile no.:

Riyadh Zaghlool Mahmood | Ph.D. | Assistant Prof.

Email: riyadh.zaghlool@uomosul.edu.iq

Mobile no.:

Mohammed Haider | M.Sc. | Assistant Lecturer

Email: mohammed.haider@uomosul.edu.iq

Mobile no.:

6. Credits, Grading and GPA

Credits

The University of Mosul 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 (50 - 100)	A - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	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	FX – Fail	راسب - قيد المعالجة	(45-49)	More work required but credit awarded

(0 – 49)	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 تقريب العلامات العشرية التي تزيد أو تقل عن ٠.٥ إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، سيتم تقريب علامة ٥٤.٥ إلى ٥٥، بينما سيتم تقريب 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 التقريب التلقائي الموضح أعلاه.

Calculation of the Cumulative Grade Point Average (CGPA)

- 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
CYBS-101	Programming (1)	78	122	8.00	C	
CYBS-102	Discrete Structures (1)	48	52	4.00	B	
CYBS-103	Logic Design Fundamentals	63	87	6.00	C	
CYBS-104	Information Security Principles	63	62	5.00	B	
CYBS-105	Calculus	48	27	3.00	S	
UOM1021	English Language (1)	32	18	2.00	S	
UOM1040	Democracy and Human Rights	32	18	2.00	S	
Total		364	386	30.00		

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-107	Advanced Programming	78	97	7.00	C	
CYBS-108	Computer Organization	78	72	6.00	C	

CYBS-109	Cyber Security Fundamentals	63	62	5.00	B	
CYBS-110	Discrete Structures (2)	48	52	4.00	B	
CYBS-111	Probabilities & Statistics	48	27	3.00	S	
UOM1011	Arabic Language (1)	32	18	2.00	S	
UOM1031	Computer	48	27	3.00	S	
Total		395	355	30.00		

Semester 3 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-201	Object-Oriented Programming (1)	78	122	8.00	C	
CYBS-202	Data Structures	63	62	5.00	B	
CYBS-203	Computational Theory	48	27	3.00	S	
CYBS-204	Database Basics	63	37	4.00	B	
CYBS-205	Cryptography (1)	78	122	8.00	C	
UOM2022	English Language (2)	32	18	2.00	S	
Total		362	388	30.00		

Semester 4 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-207	Object-Oriented Programming (2)	78	97	7.00	C	
CYBS-208	Cyber Security Tools	48	77	5.00	C	
CYBS-209	Distributed Databases	63	37	4.00	B	
CYBS-210	Software Security	48	77	5.00	B	
CYBS-211	Cryptography (2)	48	77	5.00	C	
UOM2050	Ba'ath Crimes in Iraq	32	18	2.00	S	
UOM2012	Arabic Language (2)	32	18	2.00	S	
Total		349	401	30.00		

Semester 5 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-301	Coding and Information Theory	48	102	6.00	C	
CYBS-302	Cloud Computing Principles	63	62	5.00	B	

CYBS-303	Computer Networks	63	62	5.00	B	
CYBS-304	Malicious Codes Analysis	63	87	6.00	C	
CYBS-305	Artificial Intelligence	63	37	4.00	B	
CYBS-306	Computer Architecture	48	52	4.00	B	
Total		348	402	30.00		

Semester 6 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-307	Compiler Design	63	62	5.00	C	
CYBS-308	Network Security	63	62	5.00	C	
CYBS-309	Database Security	48	77	5.00	C	
CYBS-310	Awareness and Training for Security	48	77	5.00	C	
CYBS-311	Secure Communication Protocols	48	77	5.00	C	
CYBS-312	Ethical Hacking	63	62	5.00	C	
Total		333	417	30.00		

Semester 7 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-401	Operating Systems	63	62	5.00	C	
CYBS-402	Internet of Things (IoT) Security	48	52	4.00	C	
CYBS-403	Web Applications Programming	63	62	5.00	C	
CYBS-404	Electronic Governance Security	48	52	4.00	C	
CYBS-405	Cloud Computing Security	63	62	5.00	C	
CYBS-406	Project I	47	128	7.00	C	
Total		332	418	30.00		

Semester 8 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Prerequisite
CYBS-407	Operating Systems Security	63	62	5.00	C	
CYBS-408	Web Applications Security	63	62	5.00	C	
CYBS-409	Digital Forensics	63	62	5.00	C	
CYBS-410	Intelligent Analysis of Security Threats	48	52	4.00	C	

CYBS-411	Information Risk Management	48	52	4.00	C	
CYBS-412	Project II	47	128	7.00	C	
Total		332	418	30.00		

8. **Contact**

Program Manager:

Oday Hashim Saeed Al-Wattar | Ph.D. | Assistant Prof.

Email: ahsa.alwattar@uomosul.edu.iq

Mobile no.:

Program Coordinator:

Faris Adel Hamed | Ph.D. | Assistant Prof.

Email: f.llwaah@uomosul.edu.iq

Mobile no.:



امسح الكود للوصول إلى النسخة الإلكترونية