دليل البرنامج الاكاديمي

Program Catalogue 2026-2025

First Cycle – Bachelor's Degree (B.Eng.)
,Al-Mustaqbal University
College of Engineering Technology
Cybersecurity Engineering Technologies

بكلوريوس هندسة تقنيات الامن السيبراني الدورة الاولى
جامعة المستقبل
الكلية التقنية الهندسية

دليل البرنامج الاكاديمي
Program Catalogue 2026-2025

About

The Department of Cybersecurity Engineering Technologies at the Technical Engineering College – Al-Mustaqbal University of Iraq is a specialised academic unit dedicated to studying and applying advanced methods for securing information systems and digital infrastructures. With the rapid expansion of electronic services and reliance on digital environments across all sectors, the demand for professionals capable of addressing cyber threats and safeguarding critical data has become .increasingly essential

The department prepares engineers with strong expertise in cyber defense, threat analysis, and security architecture, enabling them to design and implement effective solutions using modern tools .and technologies

The academic programme integrates theoretical foundations with hands-on practical training, allowing students to understand key cybersecurity concepts and apply them in realistic scenarios. The department also focuses on developing students' analytical and critical thinking skills, empowering them to protect complex systems and ensure the reliability and security of digital operations.

Furthermore, the department collaborates with governmental agencies, industry partners, and academic institutions to strengthen national cybersecurity capabilities and graduate highly qualified professionals who are prepared to meet the rapid advancements in the field

حول القسم

يعد قسم هندسة تقنيات الأمن السيبراني في الكلية التقنية الهندسية – جامعة المستقبل العراقية أحد الأقسام المتخصصة التي تهدف إلى دراسة أحدث تقنيات حماية المعلومات وتأمين البنى الرقمية. ومع التوسع الكبير في استخدام الأنظمة الإلكترونية والشبكات في مختلف القطاعات، برزت الحاجة الملحّة إلى كوادر قادرة على مواجهة الهجمات السيبرانية المتزايدة وتعزيز أمن البيانات الحيوية.

يسعى القسم إلى إعداد مهندسين يمتلكون معرفة واسعة بأساليب الدفاع السيبراني وتحليل المخاطر الرقمية، بالإضافة إلى تنمية قدراتهم على تصميم حلول فعّالة لمعالجة التهديدات الإلكترونية باستخدام أحدث التقنيات والأدوات.

يقدم القسم برنامجاً تعليمياً يجمع بين الجانب العلمي النظري والتطبيق العملي، مما يتيح للطلبة فهم الأسس العامة للأمن السيبراني وتطبيقها في بيئات محاكاة واقعية. كما يعمل القسم على تعزيز مهارات التفكير التحليلي والابتكار لدى الطلبة لتمكينهم من حماية الأنظمة المعقدة وضمان استمرارية العمل الرقمي بأعلى مستوى من الأمان.

ويحرص القسم على بناء شراكات فاعلة مع مؤسسات الدولة والقطاع الصناعي والجامعات، بما يسهم في دعم الجهود الوطنية في تعزيز الأمن الرقمي، وإعداد خريجين ذوي كفاءة عالية قادرين على مواجهة التطوير المتسارع في هذا القطاع الحيوي..

دليل البرنامج الاكاديمي
Program Catalogue 2026-2025

Vision
To prepare distinguished, innovative, and ethically responsible professionals with advanced scientific and technical competencies in cybersecurity engineering capable of adapting to evolving technologies and providing practical engineering solutions that serve society.

رؤية القسم
إعداد كوادر مهنية مبتكرة ومتمكنة علمياً وعملياً في مجال هندسة تقنيات الأمن السيبراني، قادرة على مواكبة التطوير المستمر وتقديم حلول هندسية قابلة للتطبيق، مع الالتزام بالسلوك الأخلاقي والمسؤولية المهنية وخدمة المجتمع.

Mission
To graduate skilled technical engineers with strong academic and professional capabilities in cybersecurity technologies by providing a modern learning environment and specialised faculty, enabling them to advance in higher education, succeed in professional practice, and contribute effectively within multidisciplinary teams..

الرسالة
تأهيل مهندسين تقنيين ذوي قدرات علمية ومهارية عالية في مجال تقنيات الأمن السيبراني، من خلال بيئة تعليمية متقدمة وكادر تدريسي متخصص، بما يمكّنهم من مواصلة مسيرتهم الأكاديمية والمهنية والعمل ضمن فرق متعددة التخصصات وتقديم خدمات فعّالة للمجتمع.

Objectives
- Apply engineering principles effectively to solve professional problems related to the design, protection, and maintenance of cybersecurity systems while considering ethical, social, and environmental implications.
- Enhance students' ability to communicate effectively with diverse and international audiences, collaborate within multifunctional teams, and assume leadership roles that meet employer expectations.
- Promote continuous engagement in professional and technical development to keep pace with advancements in cybersecurity.

الاهداف
- تطبيق المبادئ الهندسية بكفاءة لمعالجة المشكلات المتعلقة بتطوير وحماية الأنظمة السيبرانية، مع إدراك الجوانب الأخلاقية والاجتماعية والبيئية المرتبطة بذلك.
- تنمية مهارات التواصل الفعّال مع مختلف الفئات محلياً ودولياً، والعمل بروح الفريق وتحمل الأدوار القيادية لتلبية متطلبات سوق العمل.
- تعزيز المشاركة المستمرة في التطوير التقني والمهني ومتابعة المستجدات الحديثة في مجال الأمن السيبراني.

Learning Outcomes, Teaching, Learning and Assessment Methods

A. Knowledge and Understanding

:Graduates are expected to

Apply advanced knowledge in cybersecurity, network security, cryptography, ethical hacking, and .digital forensics

Demonstrate understanding of professional, ethical, and legal responsibilities in cybersecurity .practices

Evaluate course outcomes in collaboration with faculty members, cybersecurity professionals, and .industry stakeholders for continuous improvement

Exhibit leadership skills, ethical conduct, responsibility, and respect for privacy and data protec- ...tion

B. Subject-Specific Skills

:Graduates will be able to

.Work effectively within multidisciplinary cybersecurity and IT teams

.Design, implement, and evaluate secure systems, networks, and cybersecurity solutions

.Analyze cyber threats and vulnerabilities and apply appropriate defense mechanisms

.Conduct penetration testing, risk assessment, and security auditing

.Use cybersecurity tools to detect, prevent, and respond to cyberattacks

Plan, execute, and manage cybersecurity projects from design to deployment

C. Thinking Skills

:Graduates will demonstrate

.Effective communication with stakeholders in security, military, governmental, and private sectors

.Commitment to continuous learning in the rapidly evolving cybersecurity field

.Awareness of emerging cyber threats, technologies, and global security challenges

Ability to evaluate the impact of cybersecurity solutions on organizations and society

D. General and Transferable Skills

:Graduates will be able to

.Analyze and evaluate systems in relation to information security and risk management

Use modern cybersecurity tools and software to identify vulnerabilities and develop secure solu- .tions

.Present technical cybersecurity concepts clearly to non-technical audiences

.Work efficiently under pressure in high-risk and dynamic environments

Design and conduct security experiments, analyze results, and apply engineering judgment in deci- .sion-making

..

Student Learning Outcomes

The Bachelor of Science in Cybersecurity Engineering program prepares graduates for professio-
.nal careers, higher education, and research in cybersecurity and information security fields

Outcome 1: Secure Systems Development

:Graduates will be able to
Understand, design, and develop secure systems and networks using modern cybersecurity tech-
niques

.

Outcome 2: Professional Competence

:Graduates will
Compete effectively in the job market and qualify for advanced studies in cybersecurity and related fields

.

Outcome 3: Practical and Laboratory Skills

:Graduates will
Perform cybersecurity experiments, simulations, and fieldwork using modern tools while adhering to safety and ethical standards

.

Outcome 4: Scientific and Technical Knowledge

:Graduates will
Demonstrate understanding of core cybersecurity principles, theories, and evolving technologies

.

Outcome 5: Data Analysis and Threat Assessment

:Graduates will
Analyze security data, detect threats, and apply analytical techniques for incident response and prevention

.

Outcome 6: Critical Thinking and Problem Solving

:Graduates will
Apply critical thinking to identify, analyze, and solve cybersecurity challenges, and contribute to re-
.search and innovation

Job Opportunities for Graduates

Graduates of the department can work in various sectors including government, military, banking, healthcare, telecommunications, and private companies, both locally and internationally.

Examples include:
Cybersecurity Engineer
Information Security Analyst
Penetration Tester (Ethical Hacker)
Digital Forensics Analyst
Security Operations Center (SOC) Analyst
Network Security Engineer
Cybersecurity Consultant
IT Security Manager
Risk and Compliance Analyst
Malware Analyst
Cloud Security Engineer

Credits, Grading and GPA

Credits

The Cybersecurity Engineering Techniques program follows the Bologna Process and adopts the .European Credit Transfer and Accumulation System (ECTS)

.The total number of credits required for graduation is 240 ECTS
.Each academic year consists of 60 ECTS, distributed as 30 ECTS per semester
:ECTS corresponds to approximately 25 hours of student workload, including 1
Lectures and laboratory sessions
Tutorials and practical training
Self-study and assignments
Projects and examinations

This structure ensures alignment with international academic standards and facilitates student .mobility and credit transfer between universities

.

GRADING SCHEME مخطط الدرجات				
Group	**Grade**	التقدير	**Marks (%)**	**Definition**
Success Group (50 - 100)	A - Excellent	امتياز	90 - 100	Outstanding Performance
	B - Very Good	جد جدا	80 - 89	Above average with some errors
	C - Good	جد	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

Curriculum/Modules

The Department of Cybersecurity Engineering Technologies				
First stage				
code	ECTS	Semester	Module	ت
UOMU0208011	6	1	Introduction to Information System	1
UOMU0208012	6	1	Programming Essentials	2
UOMU0208013	6	1	Fundamental of Electrical Eng	3
UOMU0208014	5	1	Mathematics 1	4
UOMU0208015	5	1	Engineering Drawing	5
UOMU0000015	2	1	Democracy & Human Rights	6
30				

code	ECTS	Semester	Module	
UOMU0208021	6	2	Digital Logic Design	1
UOMU0208022	6	2	Engineering Workshops	2
UOMU0208023	6	2	Mathematics 2	3
UOMU0208024	5	2	General Physics	4
UOMU0208025	5	2	Ethics for the Information Age	5
UOMU0000009	2	2	Arabic language	6
UOMU0000003	2	2	English language	7