Middle Technical University
الجامعة التقنية الوسطى

First Cycle – Bachelor’s Degree (B.Eng.)
Department of **Cybersecurity Technology Engineering**
Electrical Engineering Technical College
Middle Technical University

بكالوريوس - هندسة تكنولوجيا الامن السيبراني (الدورة الأولى) – الكلية التقنية الهندسية الكهربائية – الجامعة التقنية الوسطى

وزارة التعليم العالي والبحث العلمي
Ministry Of Higher Education & Scientific Research
رئاسة الجامعة التقنية الوسطى
The Presidency of the Middle Technical University

Table of Contents | جدول المحتويات

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

1. Mission & Vision Statement

Vision Statement

Our Vision is to provide the community with technical, highly skilled engineers in the field of cybersecurity with a high level of efficiency, dedication, and ethical responsibility to be the vanguard of digital defense.

Mission Statement

Our mission is to Prepare a generation of technical engineers capable of protecting our organization's digital assets and information. This is achieved by employing cutting-edge technology, rigorous strategies, and a culture of continuous improvement. We educate and empower to foster a cyber-aware culture that reduces risk and ensures the success of our institutions.

2. Program Specification

Program code:	CSTE	**ECTS**	240
Duration:	4 levels, 8 Semesters	**Method of Attendance:**	Full Time

The Cybersecurity Technology Engineering Department program specification provides a comprehensive framework for the department's operation, goals, and objectives. The department offers a Bachelor of Engineering in Cybersecurity Technology Engineering, consisting of core courses in cybersecurity principles, network security, cryptography, and ethical hacking, and elective courses in specialized areas besides some foundation basic and supportive area courses.

Research and projects will focus on areas that include but are not limited to network security, information assurance, secure software development, threat intelligence, and digital forensics. The department will focus on collaborating with industry partners to facilitate internships, co-op programs, and guest lectures for students. Industry partnerships also support research projects, providing real-world relevance to the department's activities.

The department emphasizes the importance of ethical conduct in cybersecurity education and research. Students and faculty must adhere to a strict code of ethics, including respect for privacy, confidentiality, and responsible disclosure. The department regularly assesses its programs and curriculum to ensure alignment with industry standards and emerging trends. Feedback from students, alumni, and industry partners is used to enhance program quality continually.

The program specification for the Cybersecurity Technology Engineering Department serves as a guiding document to maintain high standards of education, research, and ethical practice in cybersecurity. It is subject to periodic review and updates to reflect the evolving nature of cybersecurity technology and industry demands.

The Cybersecurity Technology Engineering program is designed to provide students with the skills to improve themselves by preparing them for a career in the digital sector. The curriculum consists of an integrated set of courses that builds a solid theoretical foundation for the students. Once the foundation is established, the program develops domain-specific skills in the field of cybersecurity. Graduates from the Cybersecurity Technology Engineering Department are equipped with a strong foundation in cybersecurity principles, technologies, and practices. They are well-prepared to pursue various career paths in the field of cybersecurity. Cybersecurity Engineers/Analysts play a crucial role in safeguarding an organization's digital assets, data, and information systems from cyber threats. They utilize their knowledge and skills to proactively identify vulnerabilities, implement security measures, and respond to security incidents.

3. Program Goal

For undergraduate students pursuing a degree in Cybersecurity Technology Engineering, the following generic competencies are typically expected upon graduation:

- **Technical Knowledge:**
  - Proficiency in various operating systems (e.g., Windows, Linux, macOS).
  - Understanding of networking concepts and protocols.
  - Knowledge of programming languages (e.g., Python, C++, Java).
  - Familiarity with encryption and cryptography techniques.
  - Experience with cybersecurity tools and software (e.g., IDS/IPS, firewalls, antivirus).
  - Awareness of emerging cybersecurity threats and trends.
- **Cybersecurity Fundamentals:**
  - Understanding cybersecurity principles and best practices.
  - Knowledge of risk management and threat assessment methodologies.
  - Ability to conduct vulnerability assessments and penetration testing.
- **Security Policy and Compliance:**
  - Familiarity with cybersecurity regulations and compliance standards (e.g., GDPR, HIPAA, NIST).
  - Ability to develop and enforce security policies and procedures.
- **Incident Response and Recovery:**
  - Proficiency in incident detection and response procedures.
  - Experience in managing and mitigating security incidents and breaches.
  - Knowledge of digital forensics techniques.
- **Security Architecture and Design:**
  - Ability to design secure network and system architectures.
  - Knowledge of secure coding practices.
  - Understanding of cloud security principles.
- **Security Tools and Technologies:**

- Proficiency in using security tools like SIEM (Security Information and Event Management) systems.
- Experience with intrusion detection/prevention systems (IDS/IPS).
- Knowledge of threat intelligence platforms.

Cybersecurity Awareness and Training:

- Ability to educate and train employees on cybersecurity best practices.
- Developing and conducting security awareness programs.

Problem-solving and Analytical Skills:

- Strong analytical thinking and problem-solving abilities.
- Capacity to assess and respond to security incidents and vulnerabilities.

Continuous Learning:

- Commitment to staying up to date with the latest cybersecurity threats and technologies.
- Pursuit of certifications such as CISSP, CISM, CEH, or others as relevant to the role.

These competencies provide a solid foundation for undergraduate students in cybersecurity technology engineering. The specific curriculum and emphasis on these competencies may vary from one institution to another. Still, these skills and knowledge areas are generally considered essential for a successful career in cybersecurity.

4. Student Learning Outcomes

The Department of Cybersecurity Technology Engineering requires professionals to possess generic competencies and the technical skills and knowledge needed to perform their roles effectively. Below are some of the generic competencies needed from the Department students:

- **Problem-solving:** The ability to effectively identify and resolve complex security issues, vulnerabilities, and incidents.

- **Critical Thinking:** The capacity to analyze information, assess risks, and make informed decisions regarding cybersecurity strategies and solutions.
- **Adaptability:** Cybersecurity is a rapidly evolving field, so being open to learning new technologies and adapting to emerging threats is crucial.

- **Communication Skills:** Effective communication is vital for conveying security concerns to non-technical stakeholders, writing security policies, and collaborating with team members.

- **Teamwork:** Working collaboratively with other cybersecurity professionals, IT staff, and various departments to ensure a cohesive security posture.

- **Ethical Awareness:** Understanding the ethical considerations and responsibilities of handling sensitive data and conducting security testing.
- **Compliance Knowledge:** Awareness of relevant cybersecurity regulations, standards, and best practices ensures the organization complies with legal requirements.

- **Risk Management:** The ability to assess, prioritize, and manage cybersecurity risks to effectively protect the organization's assets.

- **Continuous Learning:** Stay updated on the latest cybersecurity trends, threats, and technologies through ongoing education and training.

- **Project Management:** Basic project management skills to effectively plan, execute, and oversee cybersecurity projects.

In conclusion, Cybersecurity Technology Engineering Department professionals must possess technical and generic competencies to excel in their roles. Analytical thinking, continuous learning, adaptability, creativity, teamwork, communication skills, project management, time management, leadership, and customer service are among the essential generic competencies required. These competencies help to enhance competence and promote good performance in the department of computer engineering techniques.

5. Academic Staff

- Dalal Abdulmohsin Hammood Ph.D. in Computer Engineering / Computer Engineering | Assistant Prof.
  Email: dalal.Hammood@mtu.edu.iq
  Mobile no.: +964 7803188416

- Mohamed Ibrahim Shujaa | Ph.D. in Computer Network Engineering | Assistant Prof.
  Email: drshujaa@mtu.edu.iq
  Mobile no.: +964 07901579766

- Oras Ahmed Shareef | Ph.D. in Electrical & Electronic Engineering/ Nanotechnology | Assistant Prof.
  Email: dr.oras@mtu.edu.iq
  Mobile no.: +964 7729721788

- Mahmoud Shuker Mahmoud | Ph.D. in Computer Engineering - Computer Networking | Lecturer
  Email: mahmoud.shukur@mtu.edu.iq
  Mobile no.: +964 7707993222

- Loay Talib Ahmed | Ph.D. in Computer Science | Lecturer
  Email: Loay.alsaffar@mtu.edu.iq
  Mobile no.: +964 7728561471

- Inas Jawad Kadhim | Ph.D. in Electrical and Computer Engineering| Lecturer
  Email: inasjk@mtu.edu.iq
  Mobile no.: +964 7717408052

- Ghalib Ahmed Salman| Ph.D. in Computer Science / Image processing | Lecturer
  Email: dr.ghalib@mtu.edu.iq
  Mobile no.: +964 7703922850

- Thair Abed Sarab| Ph.D. in Information Engineering / Information and Communications Engineering | Lecturer
  Email: thairit@yahoo.com
  Mobile no.: +964 7801667666

- Siraj Qays Mahdi | Msc. in Computer Engineering Techniques | Assistant Prof.
  Email: Siraj_qays@mtu.edu.iq
  Mobile no.: +964 7902805277

- Hala Adnan Hashim| M.Sc. in Mathematics and Computer Applications | Assistant Lecturer
  Email: hala.solomon@gmail.com
  Mobile no.: +964 7736698323

- Doaa Yousif Abdullah | M.Sc. in Computer Engineering Techniques / Computer networks and Communications | Assistant Lecturer
  Email: doaa.yousif@mtu.edu.iq
  Mobile no.: +964 7721790025

- Mustafa Ahmed Saadi | M.Sc. in Electrical and Computer Engineering | Assistant Lecturer
  Email: mustafa.ahmed.saadi@gmail.com
  Mobile no.: +964 7709644026

- Firad Fawzi Zeidan | M.Sc. in Political Science/ International Relations| Assistant Lecturer
  Email: firadfawzizeidan@gmail.com
  Mobile no.: +964 7704953268

6. Credits, Grading and GPA

Credits

Middle Technical University 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 30 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 (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:				
Number 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.				

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:

   CGPA = [(1st ^{m}odule score x ECTS) + (2nd ^{m}odule score x ECTS) + ……] / 240

7. Curriculum/Modules

Semester 1 | 30 ECTS credits | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE1101	Introduction to Information System	79	71	6.00	C	
CSTE1102	Fundamental of Electrical Eng.	79	71	6.00	C	
CSTE1103	Programming Essentials	79	71	6.00	C	
CSTE1104	Mathematics I	63	62	5.00	S	
EETC102	Engineering Drawing	63	62	5.00	S	
MTU10 0 6	Democracy & Human Rights	33	17	2.00	B	

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE1201	Digital Logic Design	79	71	6.00	C	
CSTE1202	Ethics for the Information Age	48	52	4.00	C	
CSTE1203	General Physics	79	46	5.00	S	
CSTE1204	Mathematics II	63	62	5.00	S	CSTE1104

EETC101	Engineering Workshops	64	86	6.00	S	
MTU1001	Arabic Language	33	17	2.00	B	
MTU1002	English Language (1)	33	17	2.00	B	

Semester 3 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE2101	Engineering Mathematics	63	87	6.00	S	CSTE1204
CSTE2102	Electronics Fundamentals	79	71	6.00	S	CSTE1102
CSTE2103	Linux Essentials	79	46	5.00	C	
CSTE2104	Computer Organization & Architecture	79	71	6.00	C	
CSTE2105	Data Structure & Algorithms	79	46	5.00	C	CSTE1103
MTU1007	The Crimes of the Baath regime in Iraq	33	17	2.00	B	

Semester 4 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE2201	Numerical Analysis & Statistics	63	62	5.00	S	CSTE1104, CSTE1204
CSTE2202	Object Oriented Programming	79	71	6.00	C	
CSTE2203	Microprocessors	94	56	6.00	C	CSTE2104
CSTE2204	Communication Fundamentals	79	71	6.00	C	

CSTE2205	Introduction to Database -SQL	79	46	5.00	C	CSTE2105
MTU1003	English Language (2)	33	17	2.00	B	CSTE1106

Semester 5 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE3101	Computer Network Fundamentals	79	46	5.00	C	
CSTE3102	Information Security & Cryptography	79	46	5.00	C	
CSTE3103	Digital Signal Processing	79	46	5.00	C	
CSTE3104	Software Engineering	79	46	5.00	C	
CSTE3105	Python Programming	79	46	5.00	C	
CSTE31XX	Elective I	79	46	5.00	E	

Semester 6 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE3201	Cybersecurity Essentials	79	46	5.00	C	
CSTE3202	Artificial Intelligence	79	46	5.00	C	CSTE3105
CSTE3203	Operating Systems	79	46	5.00	C	
CSTE3204	Web Design	79	46	5.00	C	
CSTE3205	Computer Network Protocols	79	46	5.00	C	CSTE2206
CSTE32XX	Elective II	79	46	5.00	E	

Semester 7 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE4101	Advanced Cybersecurity	94	56	6.00	C	CSTE3201
CSTE4102	Network Security	94	56	6.00	C	CSTE3101, CSTE3201
CSTE4103	Cloud Computing	79	71	6.00	C	
CSTE4104	Cybersecurity Governance	64	61	5.00	C	
CSTE4105	Project Preparation	33	17	2.00	S	
CSTE41XX	Elective III	79	46	5.00	E	

Semester 8 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE4201	Ethical Hacking & Penetration Testing	94	56	6.00	C	CSTE4101
CSTE4202	IoT Security	94	56	6.00	C	
CSTE4203	Mobile Security	79	46	5.00	C	
MTU1008	Professional Ethics	48	27	3.00	B	
CSTE4205	Final Project	78	47	5.00	C	
CSTE42XX	Elective IV	79	46	5.00	E	

Elective Subjects:

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CSTE3106	Digital Forensics	79	46	5.00	E	
CSTE3107	Multimedia Security	79	46	5.00	E	
CSTE3206	Wireless Networks Security	79	46	5.00	E	CSTE3101
CSTE3207	Information Theory and Coding	79	46	5.00	E	
CSTE4106	Biometric Security	79	46	5.00	E	
CSTE4107	Web Applications Security	79	46	5.00	E	CSTE3201
CSTE4206	Machine Learning Systems	79	46	5.00	E	
CSTE4207	Cloud Security	79	46	5.00	E	CSTE4103
CSTE3106	Digital Forensics	79	46	5.00	E	
CSTE3107	Multimedia Security	79	46	5.00	E	

8. Contact

Program Manager:

- Dalal Abdulmohsin Hammood | Ph.D. in Computer Engineering - Computer Engineering | Assistant Prof.
  Email: dalal.hammood@mtu.edu.iq
  Mobile no.: +964 7803188416

Program Coordinator:

- Mahmud Shuker Mahmoud | Ph.D. in Computer Engineering - Computer Networking | Lecturer
  Email: mahmoud.shukur@mtu.edu.iq
  Mobile no.: +964 7707993222

Department Coordinator:

- Hala Adnan Hashim| Msc. in Mathematics and Computer Applications | Assistant Lecturer
  Email: hala_adnan @mtu.edu.iq
  Mobile no.: +964 7736698323