Northern Technical University

الجامعة التقنية الشمالية

First Cycle – Bachelor's degree (B.Sc.) – Cybersecurity Engineering Technology

بكالوريوس هندسة تقنيات الامن السيبراني

Table of Contents | جدول المحتويات

1. Mission & Vision Statement | بيان المهمة والرؤية
2. Program Specification | مواصفات البرنامج
3. Program (Objectives) 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

The Department of Cybersecurity Engineering Technology envisions a future in which digital security is treated as a fundamental priority and cloud computing is utilized to its full potential. This vision reflects the critical importance of both fields and the distinct roles they play, with cybersecurity focused on protecting systems against unauthorized access, cyber threats, and the compromise of networks and data. The department equips students with a solid understanding of cybersecurity principles and their practical applications in both cybersecurity and cloud computing environments, enabling them to analyze security challenges and apply appropriate techniques to develop effective solutions. The program also emphasizes the ability to design, implement, and improve cybersecurity strategies to address evolving threats. Graduates are prepared to plan, implement, maintain, and monitor security measures that protect computer systems and information networks, identify vulnerabilities in digital and electronic systems, assess associated risks, and propose and apply suitable mitigation strategies. In addition, they ensure that appropriate security controls are in place to safeguard sensitive data and are capable of responding effectively to cyber incidents, including system breaches and malware attacks..

Mission Statement

The mission of the Department of Cybersecurity Engineering Technology is to play a vital role in advancing the field of cybersecurity by preparing students with the knowledge and skills required to protect systems and data from cyberattacks and security threats. The department focuses on training students in the use of modern technologies and tools to secure digital environments and ensure information integrity. Its curriculum covers key areas such as security analysis, cryptography, malware protection, identity verification, access control, network security management, and cloud computing. These subjects are delivered using up-to-date technologies and software platforms, enabling students to gain practical and relevant competencies for careers in cybersecurity and cloud computing. Overall, the department's mission is to develop qualified graduates capable of safeguarding digital systems and information assets using advanced cybersecurity methods and technologies.

2. Program Specification

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

Cybersecurity is a broad and essential discipline that plays a key role in meeting the challenges of the modern digital world. The program focuses on the full digital ecosystem, including everything from application code to the complex network infrastructures used by global organizations. It is a popular

field of study, attracting students both because of its wide scope and because it provides opportunities for later specialization. After completing the first year, students may choose to transfer into specialized degree pathways such as Network Security, Digital Forensics, or Cyber Intelligence.

Level 1 introduces students to the fundamental principles of cybersecurity and is designed to provide a foundation suitable for progression into all programs within the cybersecurity discipline. At Level 2, students begin to study core program-specific subjects that build upon this foundation. By Levels 3 and 4, students are prepared for advanced, research-informed specialist modules that deepen their expertise in chosen areas. As a result, graduates of the cybersecurity program develop an understanding of how current research influences teaching practices and industry standards, in alignment with the mission statements of the University and the College.

At Levels 2, 3, and 4, students have the flexibility to select more than half of their module credits, provided they choose a balanced range of subjects that reflect the multi-layered nature of digital security. These modules span areas such as secure coding and cryptography, network and system hardening, critical infrastructure protection, and threat intelligence, ensuring the comprehensive knowledge expected of a cybersecurity graduate. This structure enables students to pursue their individual academic and professional interests within the field. Module choices are made with guidance and support from academic advisors and personal tutors.

A strong emphasis on research and practical skills is developed from the beginning of the program through laboratory work, which is integrated into lecture-based modules or delivered as dedicated practical sessions. In addition, students participate in research seminars on emerging cyber threats as well as tutorial-based learning activities. At Level 1, students are required to complete and pass a compulsory practical security module, such as an introductory ethical hacking laboratory course, in order to progress to Level 2. In higher levels (Levels 2, 3, and 4), students may choose optional advanced modules in areas such as penetration testing and digital forensics. At Level 4, all students undertake an independent research project, which may take the form of a research or data analysis study focusing on threat trends, or a practical project conducted within a Security Operations Center (SOC) laboratory or a simulated cybersecurity environment.

Academic tutorials are conducted in Levels 1 and 2 by the same tutor, who also serves as the student's personal tutor, ensuring continuity and consistent academic support. These tutorials include a series of workshops designed to develop essential academic skills such as effective use of library resources, academic writing, and presentation techniques. Students then complete assessed tasks, such as essays and oral presentations, which allow them to apply and refine these skills within a subject-specific context.

Opportunities for international study years and industrial placements with cybersecurity organizations are also available to students. Individual career aspirations and professional development needs are discussed with academic tutors and supported wherever possible through suitable placement or study options.

3. Program Objectives

1. The program aims to produce qualified engineering graduates capable of designing and implementing secure systems that defend against cyber threats and vulnerabilities. Graduates will be able to develop and deploy secure network solutions, and transform conventional systems into secure and resilient infrastructures. They will also be equipped to manage security technologies, audit and intrusion detection systems, and conduct vulnerability assessments and penetration testing. In addition, they will understand the nature and impact of successful cyberattacks on the operational effectiveness of digital systems. Ultimately, graduates will contribute to strengthening long-term cybersecurity resilience and supporting effective response to cyber incidents at the national level.
2. Preparing engineering graduates with a high level of understanding, knowledge, and academic and technical competence, combining engineering insight, technical creativity, scientific ability, and high-quality implementation skills in the field of cybersecurity engineering technology
3. Graduating engineering cadres who are responsible for building, designing and protecting information technology systems in institutions to prevent data breaches, keep them safe from hackers, viruses and other potential problems, supervise and build network infrastructure of various types and available systems
4. Graduating engineering cadres with the scientific and technical skill that enables him to master dealing with cloud computing operations and using vulnerability examination tools to detect various technical problems, follow up on the failure and evaluation of security patches, mitigate security vulnerabilities, and provide assistance in security documentation and disaster recovery solutions.
5. Preparing engineering cadres with the technical and scientific skill that enables him to analyze data records and conduct risk assessments in the event of security breaches to know the parts of the system that have been penetrated and where the danger lies. Data breaches and secure systems to explore potential vulnerabilities in order to ensure the integrity of network systems
6. Providing experts in the field of cybersecurity to help achieve the long-term plan of the Iraqi state with the presence of experts in the field of cybersecurity.
7. Empower students with soft skills and values to communicate and collaborate effectively with others professionally, ethically and legally.
8. Ensure that students' knowledge and skills are in line with the latest cybersecurity technologies.
9. Achieving greater interaction between the Technical College of Engineering for Computer and Artificial Intelligence and the community in all its institutions for the purpose of experiencing the circumstances and reality and finding appropriate solutions to the problems.

4. Student Learning Outcomes

Cybersecurity Engineering Technology is the study of protecting digital systems, networks, and data across all layers of the computing environment, including hardware, software, and communication infrastructures. Graduates gain knowledge of the technical, historical, ethical, and societal aspects of cybersecurity and are able to apply foundational principles to understand and address complex security challenges. The program offers a Bachelor of Science in Cybersecurity Engineering Technology with emphasis areas such as Network Security, Digital Forensics, Cyber Intelligence, and Cloud Security. In addition, the department supports interdisciplinary learning by offering cybersecurity-related courses to students from other academic programs and contributing to broader engineering and computing curricula. The cybersecurity curriculum is designed to prepare students for entry into professional cybersecurity roles, graduate studies, research activities, and technical careers in areas such as security analysis, incident response, penetration testing, and security systems engineering.

Outcome 1

A. Knowledge

A. Cognitive Objectives

1. Evaluate computer systems, networks and software applications for vulnerabilities.
2. Design and implement cybersecurity measures to protect systems and data from cyberattacks.
3. Data analysis and verification of illegal activities on networks and systems.
4. Understand and deal with cloud computing concepts and applications.
5. Maintain the confidentiality and security of data and detect breaches that occur.
6. Take countermeasures to unauthorized intrusions and countermeasures through data protection skills

B. Skills objectives of the program

1. Critical thinking: The ability to analyze complex problems, evaluate different solutions, and make informed decisions based on evidence and logic is critical in cybersecurity engineering.
2. Problem-solving skills: The ability to identify security vulnerabilities, develop effective solutions, and efficiently troubleshoot problems is an essential skill for a cybersecurity engineer.
3. Analytical skills: The ability to examine data, detect patterns, and interpret trends is essential to understanding cyber threats and developing effective defensive strategies.
4. Attention to detail: Developing a keen eye on details is vital to ensure the security of systems and networks
5. Creativity: Thinking outside the box and coming up with innovative solutions to combat evolving cyber threats is a valuable skill for cybersecurity engineers
6. Risk assessment skills: The ability to assess and prioritize potential risks based on their impact and develop risk mitigation strategies is critical in cybersecurity.
7. Adaptability: Being adaptable and wanting to learn new techniques and techniques is essential to stay ahead of cyber threats.

8. Collaborative skills: Working effectively in teams, communicating ideas clearly, and collaborating with colleagues from diverse backgrounds are important skills to address complex cybersecurity challenges.
9. Continuous learning: Having a continuous learning mindset and staying up-to-date Trends and technologies are essential to succeed in this critical in cybersecurity.
7. Adaptability: Being adaptable and willing to learn new techniques and techniques is essential to stay ahead of threats

Outcome 2

Value objectives

1. Teamwork: Ability to work collaboratively with colleagues, share knowledge, and contribute effectively to group projects or incident response teams.
2. Time Management: Skill in prioritizing tasks, meeting deadlines, and efficiently managing workload to handle multiple projects simultaneously.
3. Ethical mindset: Commitment to upholding ethical standards, maintaining confidentiality, and adhering to legal regulations in cybersecurity practices.
4. Research and Commitment to Learning: A strong dedication to continuous learning and survival Updating with the latest trends is vital to success in cybersecurity.
5. Resilience: Ability to deal with high-stress situations, recover from setbacks, and persevere in finding solutions in the middle of evolving cyber threats.
6. English and Arabic speaking skills
7. Leadership and Communication: Developing leadership skills and building a professional network can enhance career opportunities and facilitate collaboration in cybersecurity.

5. Academic Staff

No	Name	Permanent/ Contract	Certificate	General	Exact	Position/responsibility
1	Hasan Kareem Abdulrahman Mohammed	Permanent	Ph.D.	Computer Science	Image Processing and Information Security	Assistant Dean for Scientific Affairs
2	Hayder Touran Mahdi Assafli	Permanent	Ph.D.	Electrical Engineering	Electronic and Communications Engineering	Head of Department
3	Abbas yuldurum saleh	Permanent	Ph.D.	Electronic and Control Engineering Technologies	Optoelectronics	Head of Rankings Unit
4	Alaan Ghazi Mohammed Ramadan	Permanent	Ph.D.	Computer Science	Communications	Assistant, Graduate Studies Division
5	Enas Faek Aziz	Permanent	Ph.D.	Computer Science	Security, Protection, and Artificial Intelligence	
6	Deniz Nisham Anwer Ismail	Permanent	M. Sc.	Computer Engineering	Computer Engineering	Department Secretary
7	Ihsan Hassan Hussein Salman	Permanent	M. Sc.	Software Engineering	Network Security	
8	Arkan Raoof Ismael Mustafa	Permanent	M. Sc.	Electrical and Electronic Engineering	Electronics	
9	Huda Hamza Abdulkhudhur Jaber	Permanent	M. Sc.	Electrical Engineering	Telecommunication	Assistant, Studies and Planning Division

10	Helen Farqad Taha Abduallah	Permanent	M. Sc.	Computer Engineering	Software	
11	Bashaar Mohammed Kulmurad mam khan	Permanent	M. Sc.	Public Law	Constitutional Law	Head of Legal Division
12	Noor Abdulsalam Fadhil Mohammed	Permanent	M. Sc.	Computer Science	Information Technology	
13	Shayma Jafar Kadhim Qasim	Permanent	M. Sc.	Control and Systems Engineering	Mechatronics Engineering	

6. Credits, Grading and GPA

Credits

Northern 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 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 (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 | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
NTU100	Democracy and Human Rights	33	17	2.00	B	
NTU101	English language	33	17	2.00	B	
CYBT108	Mathematics	63	87	6.00	S	
CYBT101	Fundamentals of Electrical Engineering	63	62	5.00	S	
CYBT103	Fundamentals of Programming	63	62	5.00	C	
CYBT100	Linux Administration	63	62	5.00	C	
CYBT109	Engineering Drawing	48	27	3.00	B	
CYBT102	Ethics of Information Age	33	17	2.00	S	

Semester 2 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
NTU102	Computer 1	48	2	2.00	B	
NTU103	Arabic Language	33	17	2.00	B	
CYBT106	Digital Electronics	63	62	5.00	S	
CYBT105	Introduction to Python Programming	63	87	6.00	C	CYBT103
CYBT104	Engineering Mathematics	48	102	6.00	S	CYBT108
CAIK100	Physics	33	42	3.00	S	
CYBT107	Introduction to Cybersecurity	63	87	6.00	C	

Semester 3 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT200	Fundamentals of Electronic Engineering	63	37	4.00	S	
CYBT205	Discrete Math	48	52	4.00	C	CYBT108
CYBT201	Database systems	63	37	4.00	C	
CYBT202	Python Programming for Cybersecurity	63	62	5.00	C	CYBT105
CYBT203	Operating Systems	48	52	4.00	C	
NTU200	Bath Party Crimes	33	17	2.00	B	
NTU201	English language	33	17	2.00	B	NTU 101
CYBT204	Computer Networks	63	62	5.00	C	

Semester 4 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT206	Data structures	37	100	4.00	C	
CYBT207	Probability & Statistics for Cybersecurity	87	150	6.00	C	CYBT104
CYBT208	Computer Organization and Architectures	62	125	5.00	S	CYBT106
CYBT209	Network Security	87	150	6.00	C	CYBT204
NTU203	Arabic Language	17	50	2.00	B	NTU103
CYBT210	Network Administration and Infrastructure	52	100	4.00	C	CYBT204
NTU202	Computer 2	27	75	3.00	B	NTU102

Semester 5 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT300	Introduction to Cryptography	63	87	6.00	C	CYBT205
CYBT301	Introduction to Hardware security	63	112	7.00	C	CYBT200, CYBT203
CYBT302	Communication Systems	33	92	5.00	S	
CYBT303	Microprocessors	63	62	5.00	S	CYBT208
CYBT304	Database security	63	62	5.00	C	CYBT201
CAIK301	Entrepreneurial Capacity Building	33	17	2.00	B	

Semester 6 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT305	Intrusion Detection and Prevention Systems	63	62	5.00	C	CYBT209
CYBT306	Cryptosystems	63	62	5.00	C	CYBT300, CYBT207
CYBT307	Operating system security	63	62	5.00	C	CYBT203
CYBT308	Mobile and Wireless Networks	63	62	5.00	C	CYBT204, CYBT302
CYBT309	Engineering Analysis	63	37	4.00	S	
CYBT310	Cloud Computing Security	63	87	6.00	C	CYBT203, CYBT210, CYBT304

Semester 7 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT400	Mobile and Wireless Networks Security	63	87	6.00	C	CYBT308
CYBT401	Research Methodology	33	42	3.00	S	
CYBT402	AI for Cybersecurity Engineering	63	87	6.00	C	
CYBT403	Ethical Hacking and Penetration Testing	63	87	6.00	C	CYBT308, CYBT100
CYBT404	Applied Cryptosystems	63	12	3.00	C	CYBT306
CYBT405	Graduation Project Design	33	117	6.00	C	

Semester 8 | 30 ECTS | 1 ECTS = 25 hrs

Code	Module	SSWL	USSWL	ECTS	Type	Pre-request
CYBT406	IT Project Management	33	117	6.00	C	
CYBT407	Graduation Project Implementation	33	42	3.00	C	CYBT405
CYBT408	Digital Forensics	63	112	7.00	C	
CYBT409	IoTs and Cybersecurity	63	112	7.00	C	
CYBT410	Reverse Engineering-Malwares Analysis	63	112	7.00	C	CYBT303, CYBT307
CYBT406	IT Project Management	33	117	6.00	C	

8. Contact

Program Manager: Program Management Committee
Email: kteccai.dep.cs@ntu.edu.iq