

Digital Transformation Electronics

Associate

TR-NQF-HE: Level 5

QF-EHEA: Short Cycle

EQF-LLL: Level 5

General course introduction information

Course Code:	MBLP251										
Course Name:	Siber Güvenlik										
Course Semester:	Fall										
Course Credits:	<table><thead><tr><th>Theoretical</th><th>Practical</th><th>Credit</th><th>ECTS</th></tr></thead><tbody><tr><td></td><td></td><td>3</td><td>5</td></tr></tbody></table>			Theoretical	Practical	Credit	ECTS			3	5
Theoretical	Practical	Credit	ECTS								
		3	5								
Language of instruction:	TR										
Course Requisites:											
Does the Course Require Work Experience?:	No										
Type of course:	Department/Faculty Elective										
Course Level:	<table><tbody><tr><td>Associate</td><td>TR-NQF-HE:5. Master`s Degree</td><td>QF- EHEA:Short Cycle</td><td>EQF-LLL:5. Master`s Degree</td></tr></tbody></table>			Associate	TR-NQF-HE:5. Master`s Degree	QF- EHEA:Short Cycle	EQF-LLL:5. Master`s Degree				
Associate	TR-NQF-HE:5. Master`s Degree	QF- EHEA:Short Cycle	EQF-LLL:5. Master`s Degree								
Mode of Delivery:	Face to face										
Course Coordinator :	Öğr.Gör. ALPER ÇELTİKÇİ										
Course Lecturer(s):	Öğr.Gör. AHMET TOSUNOĞLU										
Course Assistants:											

Course Objective and Content

Course Objectives:	The aim of this course is to introduce students to the basic concepts of information and cyber security, to identify common threats and vulnerabilities, to teach basic cryptographic principles, network security mechanisms and the importance of security policies.
Course Content:	Basic principles of information security (CIA), common cyber attacks (Phishing, Malware, DoS), introduction to cryptography (symmetric/asymmetric encryption, hash), network security (Firewall,

IDS/IPS), web application security (SQL Injection, XSS), security policies and ethical hacking basics.

Learning Outcomes

The students who have succeeded in this course;

Learning Outcomes

1 - Knowledge

Theoretical - Conceptual

- 1) It defines the basic principles of information security (Confidentiality, Integrity, Accessibility - CIA).
- 2) Explain the common types of cyberattacks and their motivations.
- 3) Simetrik ve asimetrik şifrelemenin temel çalışma mantığını karşılaştırır.
- 4) It lists the key tools used for network security and their functions.
- 5) In a simple risk analysis scenario, it identifies assets, threats, and vulnerabilities.

2 - Skills

Cognitive - Practical

3 - Competences

Communication and Social Competence

Learning Competence

Field Specific Competence

Competence to Work Independently and Take Responsibility

Lesson Plan

Week	Subject	Related Preparation
1)	Introduction to Cybersecurity: Basic Concepts, CIA Triangle	-
2)	Threats, Vulnerabilities and Risk Management	-
3)	Malware: Viruses, Worms, Ransomware	-

4)	Social Engineering and Phishing Attacks	-
5)	Introduction to Cryptography: Symmetric and Asymmetric Cryptography, Hash Functions	-
6)	Authentication and Access Control Mechanisms	-
7)	Network Security Basics: TCP/IP Vulnerabilities, Firewalls	-
8)	Midterm Exam	-
9)	Intrusion Detection and Prevention Systems (IDS/IPS)	-
10)	Web Application Security: SQL Injection, XSS	-
11)	Wireless Network Security (WEP, WPA/WPA2/WPA3)	-
12)	Security Policies and Standards (ISO 27001)	-
13)	Ethical Hacking and Penetration Testing Methodologies	-
14)	Introduction to Incident Response and Forensics	-
15)	Final Exam	-

Sources

Course Notes / Textbooks:	-
References:	-

Course-Program Learning Outcome Relationship

Learning Outcomes	1	2	3	4	5
Program Outcomes					
1) Explains the fundamental principles of electrical, electronic, and digital circuits.					
2) Constructs and analyzes analog/digital circuits and applies proper measurement techniques.					
3) Develops embedded system applications using algorithm and programming knowledge.					
4) Designs sensor, transducer, and IoT-based data acquisition and communication systems.					

5) Analyzes and interprets analog and digital signals with signal processing techniques. Learning Outcomes	1	2	3	4	5
6) Implements automation applications using PLCs, robotics, and industrial control components.					
7) Applies digital transformation processes, data management, and AI/machine learning techniques.					
8) Explains and applies network fundamentals, communication protocols, and cybersecurity principles.					
9) Communicates effectively in teams, applies project management methods, and acts according to professional ethics.					
10) Solves technical problems in real workplace settings, assumes responsibility, and demonstrates readiness for lifelong learning.					

Course - Learning Outcome Relationship

No Effect	1 Lowest	2 Low	3 Average	4 High	5 Highest

	Program Outcomes	Level of Contribution
1)	Explains the fundamental principles of electrical, electronic, and digital circuits.	
2)	Constructs and analyzes analog/digital circuits and applies proper measurement techniques.	
3)	Develops embedded system applications using algorithm and programming knowledge.	
4)	Designs sensor, transducer, and IoT-based data acquisition and communication systems.	
5)	Analyzes and interprets analog and digital signals with signal processing techniques.	
6)	Implements automation applications using PLCs, robotics, and industrial control components.	
7)	Applies digital transformation processes, data management, and AI/machine learning techniques.	
8)	Explains and applies network fundamentals, communication protocols, and cybersecurity principles.	
9)	Communicates effectively in teams, applies project management methods, and acts	

	according to professional ethics.	
10)	Solves technical problems in real workplace settings, assumes responsibility, and demonstrates readiness for lifelong learning.	

Learning Activity and Teaching Methods

Expression	✓
Problem Solving	✓
Q&A / Discussion	✓
Case Study	✓

Assessment & Grading Methods and Criteria

Written Exam (Open-ended questions, multiple choice, true-false, matching, fill in the blanks, sequencing)	✓
Homework	✓
Case study presentation	✓

Assessment & Grading

Semester Requirements	Number of Activities	Level of Contribution
Midterms	1	% 40
Final	1	% 60
total		% 100
PERCENTAGE OF SEMESTER WORK		% 40
PERCENTAGE OF FINAL WORK		% 60
total		% 100

Workload and ECTS Credit Grading

Activities	Number of Activities	Duration (Hours)	Workload
Course Hours	13	3	39
Study Hours Out of Class	13	3	39
Midterms	1	30	30

Final	1	30	30
Total Workload			138