

**Vocational School / Computer Programming**

**2024 - 2025 Academic Year**

**CYBER SECURITY**

**Syllabus**

<b>Course Description</b>					
<b>Name</b>	<b>Code</b>	<b>Semester</b>	<b>T+A Hour</b>	<b>Credit</b>	<b>ECTS</b>
CYBER SECURITY	BPR2166360	Fall Semester	3+0	3	5
<b>Prerequisites Courses</b>					
<b>Recommended Elective Courses</b>					
<b>Language of Instruction</b>	Turkish				
<b>Course Level</b>	Short Cycle (Associate's Degree)				
<b>Course Type</b>	Elective				
<b>Course Coordinator</b>	Lect. Beyza KOYULMUŞ				
<b>Name of Lecturer(s)</b>	Lect. Beyza KOYULMUŞ				
<b>Assistant(s)</b>					
<b>Aim</b>	Aims to inform and develop information systems, network security, computer security, software security and security vulnerabilities of computer networks against security threats encountered in computer networks, to understand the threats and measures to be taken against cyber attacks.				
<b>Course Content</b>	This course contains; Introduction to the Course and General Information about the Course Objectives, Introduction to Security,Basic Security Concepts,Introduction to Cryptology,Types of Encryption,Network security; firewalls, intrusion detection and prevention systems,Network security; firewalls, intrusion detection and prevention systems-2,Secure Software Development,Security of Web Applications,Infiltration Trials,Investigation of Malicious Software,Network Security,Security Technologies and Security Models,Project Presentations,Project Presentations.				
<b>Course Learning Outcomes</b>		<b>Teaching Methods</b>	<b>Assessment Methods</b>		
Explains basic security concepts.		10, 12, 14, 16, 19, 3, 5, 6, 8, 9	A, E, F		
Defines the concepts of cryptology.		12, 2	A, E, F, G		
Ağ güvenliği; güvenlik duvarları, saldırı tespit ve önleme sistemlerini bilir.		14, 6, 9	A, E		
Develop secure software.		14, 6, 8, 9	A, E, F		
Analyzes malicious software.		14, 6, 9	A, E, F		
Uses security technologies and security models.		14, 6, 8, 9	A, E		
<b>Teaching Methods</b>	10: Discussion Method, 12: Problem Solving Method, 14: Self Study Method, 16: Question - Answer Technique, 19: Brainstorming Technique, 2: Project Based Learning Model, 3: Problem Baded Learning Model, 5: Cooperative Learning, 6: Experiential Learning, 8: Flipped Classroom Learning, 9: Lecture Method				
<b>Assessment Methods</b>	A: Traditional Written Exam, E: Homework, F: Project Task, G: Quiz				
<b>Lecture Schedule</b>					
<b>Sequenc e</b>	<b>Topics</b>	<b>Preliminary Preparation</b>			
1	Introduction to the Course and General Information about the Course Objectives, Introduction to Security				
2	Basic Security Concepts				
3	Introduction to Cryptology				
4	Types of Encryption				
5	Network security; firewalls, intrusion detection and prevention systems				
6	Network security; firewalls, intrusion detection and prevention systems-2				
7	Secure Software Development				
8	Security of Web Applications				
9	Infiltration Trials				
10	Investigation of Malicious Software				
11	Network Security				
12	Security Technologies and Security Models				
13	Project Presentations				
14	Project Presentations				
<b>Evaluation Methods</b>		<b>Weight(%)</b>			
Midterm Exam		40			
General Exam		60			

<b>Resources</b>