

Course Description					
Name	Code	Semester	T+A Hour	Credit	ECTS
INTRODUCTION to INFORMATION SECURITY	COE4115374	Fall Semester	3+0	3	6
Prerequisites Courses	MÜHENDİSLER İÇİN PROGRAMLAMA				
Recommended Elective Courses	Data Communications and Networking				
Language of Instruction	English				
Course Level	First Cycle (Bachelor's Degree)				
Course Type	Elective				
Course Coordinator	Prof.Dr. Selim AKYOKUŞ				
Name of Lecturer(s)	Lect.Dr. Arzu KİLİTÇİ CALAYIR				
Assistant(s)	Teaching assistant				
Aim	Understand the players in the cybersecurity world and the motivation of cyber criminals and cybersecurity specialists. Learn to identify security attacks, symptoms, processes, and countermeasures. Learn foundational knowledge in various security domains. Build skills in security management, controls, protection, and mitigation technologies. Learn security laws, ethics, and how to develop security policies. Learn the roles of different cybersecurity professionals and career options.				
Course Content	This course contains; Cybersecurity World and Its need.,Attacks, Concepts and Techniques.,Protecting Data, Privacy, and Organization.,Cybersecurity Threats, Vulnerabilities and Attacks.,The Art of Protecting Secrets.,The Art of Ensuring Integrity.,Protecting Cyber Security Domain.,Midterm,The Five Nines Concept.,Information Security Framework.,Security Life Cycles.,Physical and Environmental Security,Disaster Recovery and Business Continuity Management.,Review of all topics covered. ,Project Presentations.				
Course Learning Outcomes			Teaching Methods	Assessment Methods	
1. Describe how the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.			10, 12, 17, 2, 3, 9	A, E, F	
2. Describe the tactics, techniques and procedures used by cyber criminals.			10, 12, 17, 2, 3, 9	A, E, F	
3. Describe how technologies, products and procedures are used to protect confidentiality and ensure integrity.			10, 12, 17, 2, 3, 9	A, E, F	
4. Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.			10, 12, 17, 2, 3, 9	A, E, F	
5. Explain the purpose of laws related to cybersecurity.			10, 12, 17, 2, 3, 9	A, E, F	
6. Describe the ISO/IEC27001 international standard for information security: Information Security Management System			10, 12, 17, 2, 3, 9	A, E, F	
Teaching Methods	10: Discussion Method, 12: Problem Solving Method, 17: Experimental Technique, 2: Project Based Learning Model, 3: Problem Baded Learning Model, 9: Lecture Method				
Assessment Methods	A: Traditional Written Exam, E: Homework, F: Project Task				
Lecture Schedule					
Sequence	Topics	Preliminary Preparation			
1	Cybersecurity World and Its need.	NetAcad C1 Ch.1			
2	Attacks, Concepts and Techniques.	NetAcad C1 Ch.2			
3	Protecting Data, Privacy, and Organization.	NetAcad C1 Ch.3			
4	Cybersecurity Threats, Vulnerabilities and Attacks.	NetAcad C1 Ch.2 & Ch. 3			
5	The Art of Protecting Secrets.	NetAcad C2 Ch.4			
6	The Art of Ensuring Integrity.	NetAcad C2 Ch.5			
7	Protecting Cyber Security Domain.	NetAcad C2 Ch.7			
8	Midterm	All topics till Week 7			
9	The Five Nines Concept.	NetAcad C2 Ch.6			
10	Information Security Framework.	Textbook Ch.2 & ch.3			
11	Security Life Cycles.	Textbook Ch.4			
12	Physical and Environmental Security	Textbook Ch.7			
13	Disaster Recovery and Business Continuity Management.	Textbook Ch.8.			
14	Review of all topics covered.	NetAcad & Textbook			
15	Project Presentations	Lecture notes, the textbook and NetAcad.			
Evaluation Methods		Weight(%)			
Midterm Exam		30			
General Exam		70			

Resources
1. Cisco NetAcad Introduction to Cybersecurity, Cisco NetAcad Cyber Essentials v1.1, and 2. Information Security Management Principles 3rd edition ISBN-10 : 1780175183Lecture presentations.