

İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı			Course Name		
Bilgi Güvenliği Yasa ve Politikaları			Information Security Law and Policy		
Kodu (Code)	Yarıyılı (Semester)	Kredisi (Local Credits)	AKTS Kredisi (ECTS Credits)	Ders Seviyesi (Course Level)	
BGK 513	Güz/Bahar (Fall/Spring)	3	7,5	Y.L. (M.Sc.)	
Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)				
Dersin Türü (Course Type)	Seçmeli (Elective)		Dersin Dili (Course Language)	Türkçe/İngilice (Turkish/English)	
Dersin İçeriği (Course Description)	Ulusal ve uluslararası geçerliliği olan bilgi güvenliği yasalarının tanıtımı ve karşılaştırılması, hukuk ve etiğin temel ilkeleri, kamusal kurallar, Özel kurallar, Ulusal güvenlik, Bireysel bilginin mahremiyeti, Fikri mülkiyet, Ahlak ve kültür. Genel ceza yasaları, Kovuşturma, Delil toplama, Adli bilişim				
<u>30-60 kelime arası</u>	Introduction and comparison of national and international policies, fundamental principles of law and ethics, public and private rules, national security, privacy of personal data, intellectual property, ethics and culture, criminal law, prosecution, evidence collection, informational forensics				
Dersin Amacı (Course Objectives)	<ul style="list-style-type: none">Bilgi güvenliği mevzuatı konusunda hukuki temellerin anlatılmasıBilgi güvenliğinin yasal kapsamıBilgi güvenliğinin hukuka etkileri				
<u>Maddeler halinde 2-5 adet</u>	<ul style="list-style-type: none">Introduction to information security legislation and policyCoverage of information security lawThe effects of information security to law				
Dersin Öğrenme Çıktıları (Course Learning Outcomes)	Öğrenciler				
<u>Maddeler halinde 4-9 adet</u>	1. Bilgi güvenliği konusundaki yasal mevzuatı 2. Mevzuatın getirdiği sorumlulukları 3. Bilgi güvenliğinde kullanılan yöntemlerin hukuka etkilerini 4. Tartışmalı yasal konuları Öğreneceklerdir.				
	Students will learn the following: 1. Legislation and law on information security 2. Liability of legislation 3. Effects of information security topics to law 4. Controversial legal topics				

Kaynaklar (References) <i>En önemli 5 adedini belirtiniz</i>	<ol style="list-style-type: none"> 1. Legal Issues In Information Security, Joanna Lyn Grama, 2010, Jones & Bartlett Learning. 2. Principles of Information Systems Security: Texts and Cases, Gurpreet Dhillon, 2006, Wiley. 3. Readings & Cases in Information Security: Law & Ethics, Michael E. Whitman, Herbert J. Mattord, 2010, Cengage Learning. 4. Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists, Thomas J. Shaw, 2012, American Bar Association. 5. Information Security Policies and Procedures: A Practitioner's Reference, 2nd Ed., Thomas R. Peltier, 2004, Auerbach Publications. 		
Ödevler ve Projeler (Homework & Projects)	1 Dönem Ödevi		
	1 Term Paper		
Laboratuvar Uygulamaları (Laboratory Work)	--		
	--		
Bilgisayar Kullanımı (Computer Use)	--		
	--		
Diğer Uygulamalar (Other Activities)	--		
	--		
Başarı Değerlendirme Sistemi (Assessment Criteria)	Faaliyetler (Activities)	Adedi* (Quantity)	Değerlendirmedeki Katkısı, % (Effects on Grading, %)
	Yıl İçi Sınavları (Midterm Exams)	1	% 30 (30 %)
	Kısa Sınavlar (Quizzes)	-	-
	Ödevler (Homework)	-	-
	Projeler (Projects)	-	-
	Dönem Ödevi/Projesi (Term Paper/Project)	1	% 30 (30%)
	Laboratuvar Uygulaması (Laboratory Work)	-	-
	Diğer Uygulamalar (Other Activities)	-	-
	Final Sınavı (Final Exam)	1	% 40 (40%)

*Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Dersin kapsamı ve giriş	
2	Hukukun temel ilkeleri	
3	Bağlayıcı yasal metinler	
4	Uluslararası bilgi güvenliği yasaları ve uygulamaları	
5	Uluslararası bilgi güvenliği yasaları ve uygulamaları	
6	Ulusal bilgi güvenliği yasaları	
7	Tartışmalı yasal konular	
8	Ulusal güvenlik açısından bilgi güvenliği mevzuatı	
9	Etik değerler açısından bilgi güvenliği mevzuatı	
10	Fikri mülkiyet açısından bilgi güvenliği mevzuatı	
11	Mahremiyet açısından bilgi güvenliği mevzuatı	
12	Bilgi güvenliği mevzuatında kovuşturma ve cezalar	
13	Delil elde etme ilkeleri	
14	Adli bilişim	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Course outline	
2	Fundamental principles of law	
3	Restrictive legal texts	
4	International computer security law and their applications	
5	International computer security law and their applications	
6	National computer security law	
7	Controversial legal issues	
8	Information security legislation from national security perspective	
9	Information security legislation from ethic perspective	
10	Information security legislation from intellectual property perspective	
11	Information security legislation from privacy perspective	
12	Prosecution and penalties in information security legislation	
13	Principles of evidence collection	
14	Informational forensics	

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracığı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).	X		
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).		X	
iii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).		X	
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).	X		
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümlenebilir (beceri).			
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).		X	
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümledikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).	X		
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).	X		

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (MS) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).	X		
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).		X	
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).		X	
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).	X		
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).			
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).			
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Cybersecurity Engineering and Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).		X	
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).	X		
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).	X		

1: Little, 2. Partial, 3. Full

<u><i>Düzenleyen (Prepared by)</i></u> Prof. Dr. Eşref ADALI	<u><i>Tarih (Date)</i></u> 31.03.2014	<u><i>İmza (Signature)</i></u>
---	--	--------------------------------