

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 1 / 6
---	--	---

## 1. AMAÇ

Bilgi Güvenliği Yönergesi'nin amacı, kurumsal bilgi güvenliği ilkelerini ana hatlarıyla belirlemek ve Üniversite'de bilginin işleme yöntemlerinin güvenli olarak gerçekleştirilmesini sağlayacak düzenlemeleri ortaya koymak, programları, verileri, iletişim ağını ve ekipmanları (donanım) kayıplara, yanlış kullanıma ve ihlallere karşı koruma altına almak, Üniversite bilgi güvenliğini tehdit edebilecek olayların oluşmasını engellemek ve bilgi güvenliği konusunda farkındalığı sağlamaktır.

## 2. KAPSAM

Tüm Koç Üniversitesi (KU) mensuplarını, mezunlarını, hizmet sağlayıcıları ve tedarikçilerini, Üniversite ile çalışan tüm üçüncü şahısları, kampüs içerisinde ikamet eden tüm bireyleri/ziyaretçileri ve bütün Bilgi Teknolojileri varlıkları ve bileşenleri kapsamaktadır.

## 3. REFERANSLAR

- 3.1. Kabul Edilebilir Kullanım Yönergesi
- 3.2. YÖK Öğrenci Disiplin Yönetmeliği
- 3.3. Koç Üniversitesi İdari Personel Yönetmeliği
- 3.4. COBIT.2019 kapsamında "Süreç, Organizasyonel Yapılar, Bilgi Akışları ve Varlıkları, İnsanlar, Beceriler ve Etkinlikler, Politikalar ve Prosedürler, Kültür, Etik ve Davranış, Hizmetler, Altyapı ve Uygulamalar" yönetim bileşenlerinin ilgili yönetim ve yönetim hedefine uygulanabilecek her biri.
- 3.5. ISO 27000: 2018 Bilgi Güvenliği yönetim standartları ailesi tamamı.
- 3.6. SANS-CIS kontrolleri (En yaygın ve tehlikeli saldırıları durdurmak için belirli ve uygulanabilir yollar sağlayan, siber güvenlik eylemler dizisidir.)
- 3.7. 5651: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 3.8. 6698: Kişisel Verilerin Korunması Kanunu
- 3.9. 4857: İş Kanunu
- 3.10. 2547: YÖK Kanunu
- 3.11. 5237: Türk Ceza Kanunu
- 3.12. 5846: Fikir ve Sanat Eserleri Kanunu

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 2 / 6
---	--	---

#### 4. SORUMLULUKLAR

- 4.1. Bu yönergenin uygulanmasından Rektör sorumludur.
- 4.2. Yönergenin oluşturulmasından, iyileştirme takibinin yapılmasından ve güncellenmesinden Bilgi Teknolojileri Direktörlüğü sorumludur.
- 4.3. Güvenlik politikalarını, yöntemlerini belirlemekten ve değerlendirmekten, Bilgi Güvenliği konusundaki özel durumların değerlendirilmesi ve uygulama esaslarının belirlenmesinden Bilgi Güvenliği Komitesi sorumludur.

#### 5. TANIMLAR

- 5.1. **Birimler:** Bilgi Teknolojileri dışında kalan tüm birimleri ifade etmektedir.
- 5.2. **Yönerge:** Bilgi Güvenliği Yönergesi
- 5.3. **KU Mensupları:** İdari çalışanlar, akademik çalışanlar, öğrenciler.
- 5.4. **Bilgi Sistemleri:** Üniversite'nin sahip olduğu, kiraladığı, uyarladığı, muhafaza altına aldığı veya kontrolü altında olan kaynakları; bu kapsamda kişisel veya kurum tarafından sağlanan bilgisayarları, ağları, bulut ve internet temelli hizmetleri, taşınabilir cihaz/depolama aygıtlarını, yazılımları ve bunlar ile ilgili her türlü donanım, teçhizat ve fikri mülkiyeti ifade eder.
- 5.5. **Bilgi Teknolojileri Varlıkları ve Bileşenleri:** Bilgisayar dosyaları ve veri tabanları, veri saklama ortamlarını, bilgi sistemlerinde üretilen tüm raporları, bilgisayar uygulama ve yazılımları ile bunlara ait dokümanları, tüm e-posta mesajlarını, veri iletim araçlarını, Üniversite'ye ait iletişim ağlarını, personel, çevresel ve fiziksel alanları, veri içeren tüm fiziksel dokümanları, tüm kurumsal süreçler/işleyiş ve yöntemleri, dış kurum ve şahıslarla ilişkileri ve sözleşmeleri, Üniversite'nin tabii olduğu bilgi güvenliğine ilişkin mevzuata uyumu ifade eder.
- 5.6. **Bilgi Güvenliği Komitesi:** Bilgi güvenliği risklerini azaltma ve güvenlik konularında tavsiyelerde bulunmak, güvenlik politikalarını belirlemek, yeni tehditleri değerlendirmek, Kişisel Verilerin Korunması Kanunu vb. regülasyonlara uyumu sağlamakla sorumlu olan üst komitedir.
- 5.7. **Bilgi Güvenliği Ekibi:** Bilgi Teknolojileri Direktörlüğü altında bulunan Üniversitenin Bilgi güvenliği süreçlerinin işletilmesinden sorumlu ekiptir. Bilgi Güvenliği Ekibi faaliyetlerini Bilgi Güvenliği Komitesine raporlamakla sorumludur. Bilgi Güvenliği Ekibine [it.ku.edu.tr](http://it.ku.edu.tr) sayfasından erişilebilir. Ekibin e-posta adresi [bilgiguvenligi@ku.edu.tr](mailto:bilgiguvenligi@ku.edu.tr) şeklindedir.

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 3 / 6
---	--	---

## 6. TEMEL PRENSİPLER

- 6.1.** KU BT direktörlüğü tarafından kullanılan ve oluşturulan bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması temel amacına yönelik olarak; üniversitenin kurumsal vizyonu ve misyonu doğrultusunda ISO/IEC 27001:2013 ile uyumlu Bilgi Güvenliği Yönetim Sistemi (BGYS) işletilmesi ile aşağıdaki kazanımların elde edilmesi hedeflenmektedir:
- 6.1.1.** Kurumsal saygınlığın artırılması
  - 6.1.2.** Hizmet kalitesinin artırılması
  - 6.1.3.** Bilgi güvenliği farkındalığını artırılması
  - 6.1.4.** Olası riskleri sınırlandırılması.
- 6.2.** Bilgi Güvenliği Yönetim Sisteminin yürütülmesi ve raporlanmasından Bilgi Güvenliği Ekibi Sorumludur. Bilgi güvenliği ekibinin faaliyetleri, görevler ayrılığı gözetilerek iç ve dış denetim ekibi tarafından denetlenmektedir.
- 6.3.** Bilgi Güvenliği Yönetim Sisteminin çıktıları Bilgi Güvenliği Komitesine raporlanır. Bilgi Güvenliği Yönetim Sisteminin uygulatılmasından ve yapılan değişikliklerin onaylanmasından Bilgi Güvenliği Komitesi sorumludur.
- 6.4.** Bu yönerge ve bağlantılı diğer yönerge ve prosedürlerin ihlal edilmesi veya ihlal edilmesine sebep olunması halinde KU İdari personeli için 4857 Sayılı İş Kanunu ve Koç Üniversitesi İdari Personel Yönetmeliği, KU Akademik personel için 2547 Sayılı YÖK Kanunu, öğrenciler için YÖK Öğrenci Disiplin Yönetmeliği işletilir.
- 6.5.** Bilgi güvenliği yönergesi kapsamında bilgi güvenliği ile ilgili uygulanabilir şartların karşılanması ve bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesi taahhüt edilir.
- 6.6.** Bilgi Güvenliği Yönergesi, Üniversite bilgi güvenliği gereksinimlerine uygun şekilde hareket edilmesi konusunda kullanılan tüm yönerge ve prosedürlere temel ve destekleyici niteliktedir. Bilgi Güvenliği gerekliliklerini sağlamak, yönetimini gerçekleştirmek için ilgili tüm süreçler dokümanite edilmiştir. (EK-1 Bilgi Güvenliği Dokümanları)
- 6.7.** Bilgi Güvenliği Yönergesi ve güncellemeleri intranet/internet üzerinden yayımlanır.

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 4 / 6
---	--	---

- 6.8.** Bilgi Güvenliği 'ne ilişkin kural ve prosedürlerin, kağıt veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilişim ve bilgi işlem sistemlerinin kullanımı için dikkate alınması esastır.
- 6.9.** Üniversite tarafından sunulan her türlü bilişim ve bilgi işlem sistemi ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün, aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça Üniversite'ye aittir.
- 6.10.** Uyulması gereken genel kullanım kuralları, Üniversite Kabul Edilebilir Kullanım Yönergesi içerisinde tanımlanmıştır.

**6.11. Doküman Güncelleme Şartları**

Bilgi Güvenliği Yönergesi'nin güncellenmesi için yeterli şartlar aşağıdaki gibidir:

- 6.11.1.** Sistem bileşenlerinde büyük değişiklik olması,
- 6.11.2.** Yeni tipte güvenlik ihlallerinin çıkması,
- 6.11.3.** Mevzuatta, kurumsal süreçlerde ya da işletim talimatlarında değişiklik yapılması,
- 6.11.4.** Güvenlik gereksinimlerinde değişiklik olması,
- 6.11.5.** Güvenlik ihlalleri,
- 6.11.6.** Bilgi Teknolojileri ve Rektörlüğün ihtiyaç duyduğu diğer tüm haller
- 6.11.7.** Bilgi Güvenliği Yönergesi gözden geçirilirken aşağıda listelenen hususlar özellikle göz önünde bulundurulur:
- 6.11.7.1.** Mevcut yönergenin etkinliği ve yeterliliği,
- 6.11.7.2.** Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri,
- 6.11.7.3.** Teknolojideki değişiklikler

**6.12. Bilgi Güvenliği Yönergesinin İhlali**

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Yönergesi'nin ihlal edildiği sonucuna varılır:

- 6.12.1.** Kasten ya da ihmal sonucu Bilgi Güvenliği Yönergesi'nde ve/veya ilgili alt yönergeler, prosedürler, teknik prosedürler ve standartlarda açıkça belirtilmiş maddelere karşı hareket etmek,
- 6.12.2.** Üniversite'nin itibarını riske atmak,
- 6.12.3.** Üniversite bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak Üniversite'yi fiili ve olası tehlike, zarar ve iş kaybına maruz bırakmak,

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 5 / 6
---	--	---

- 6.12.4.** Üniversite'nin bilgilerini yetkisiz bir şekilde kullanmak, ifşa etmek, değiştirmek, tahrip etmek ve/veya bu bilgileri izinsiz bir şekilde üçüncü kişilerle yazılı/elektronik olarak herhangi ortamda paylaşmak,
- 6.12.5.** Üniversite bilgi varlıklarını yasal olmayan bir amaç için kasten ya da ihmal sonucu kullanmak,
- 6.12.6.** Üniversite, Bilgi Güvenliği Yönergesi'nin ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak Yönerge'ye uymama veya kasıtlı Politika ihlalleri, disiplin cezası, yazılı kınama, işten çıkarma veya hukuki ve/veya cezai işlemlerle sonuçlanabilir. Üniversite, ihlalin ciddiyetine göre, ilgili kişinin sistemlere erişim haklarını ve ilgili sorumluluklarını askıya alabilir veya sonlandırabilir.

**6.13.** Bu yönergeye dair tüm tanım dışı konular ancak Bilgi Güvenliği Komitesi onayı ile uygulanır.

## 7. YÖNTEM

- 7.1.** İlki işe başlangıçta zorunlu olmak üzere, tüm KU mensuplarına yılda en az 1 (bir) kez Bilgi Teknolojileri Direktörlüğü tarafından hazırlanan bilgi güvenliği eğitimi yapılır ve yapılan eğitimler ölçümlenir.
- 7.2.** Üniversite, bağlı bulunduğu sektörel düzenlemeler ve bilgi güvenliğine yönelik kontrollerin artırılması amacıyla iç ve dış denetim faaliyetlerini gerçekleştirir.
- 7.3.** Yılda en az 1 (bir) kere olmak üzere üçüncü taraflara sızma testi yaptırılır.
- 7.4.** Bilgi Güvenliği Yönergesi'ne uyulmamasının veya ihlal edilmesinin tespiti halinde Bilgi Güvenliği Komitesi'ne bilgi verilir.
- 7.5.** BGYS süreçleri ve uyum Risk Yönetimi Uyum ve İç Kontrol Direktörlüğü tarafından denetlenmektedir.

## 8. EKLER VE KAYITLAR

EK-1 Bilgi Güvenliği Dokümanları

 <b>KOÇ ÜNİVERSİTESİ</b>	<b>BİLGİ GÜVENLİĞİ YÖNERGESİ</b> Y21-BT-001	Tarih : 25.01.2021 Güncelleme No : 2 Güncelleme Tarihi : 15.08.2022 Sorumlu Birim : BT Direktörlüğü Sayfa : 6 / 6
---	--	---

## 9. GÖZDEN GEÇİRME

Bu dokümanı gözden geçirme ve güncelleştirme sorumluluğu Bilgi Teknolojileri Direktörlüğü'ne aittir. Gözden geçirme en az yılda 1 defa yapılır. Gerekli görüldüğü zaman ve durumlarda dokümanın da revize edilmesi gereklidir.

## 10. DEĞİŞİKLİK/ DAĞITIM TABLOSU

Değişen sayfa	Tarih	Değişiklik	Değişikliği yapan
-	09.02.2022	Gözden geçirme yapılmıştır. Değişiklik yoktur.	-
6	15.08.2022	Temel prensipler başlığı altına BGYS sorumluluklar ve amaçlar eklenmiştir.	Ertuğrul Doğan
<b>Dağıtım (İlgili Bölümler)</b>			
Tüm Koç Üniversitesi			