

# FIT-S13002-01 - Internet ve Kurumsal Veri Kullanımı

Güncelleme tarihi: 20.02.2018

## 1. KAPSAM ve TANIMLAR

Bu belgenin amacı Sabancı Üniversitesi tarafından sağlanan iletişim ortamı, bilgisayar, uygulama yazılımları, web sitesi ve sayısal ortamlarda saklanan bilgi, belge, veritabanı gibi Bilgi Teknolojisi (BT) olanaklarının kullanımında dikkat edilmesi gerekenleri açıklamaktır. İşbu belgede Sabancı Üniversitesi "Üniversite", Üniversite'deki görevi gereği, nereden ve ne şekilde eriştiğine bakılmaksızın BT olanaklarını kullanan paydaşlar "kullanıcı" olarak anılacaktır.

### 1.1. Kurumsal Bilgi ve Yetkilendirme

Aksi özellikle belirtilmedikçe, Üniversite idari ve akademik süreçleri paralelinde ortaya çıkan, çeşitli ortam ve yöntemlerle erişime açılan, izinsiz paylaşılmayan, kaybı veya üçüncü şahıslar ile paylaşılması sonucunda kurumsal zarara veya itibar kaybına yol açan tüm bilgi, rapor, yazılım kodu, veritabanı kaydı ve belgeler "Kurumsal Bilgi" olarak addedilir. Bu kapsamda öğrenci ve çalışanlara ait tüm kişisel veriler, yazılım kodları, mali bilgiler, resmi belgeler, anlaşmalar, yönerge, prosedür ve proje belgeleri örnek olarak verilebilir. Görevi gereği kurumsal veri üreten, kullanan ve olması gerektiği oranda paylaşan kullanıcılar, ilgili sistem, bilgisayar, uygulama ve iletişim ağında özel olarak yetkilendirilirler. Yetkileri oranında iş gören kullanıcılar; bu belgede, ilgili Üniversite yönetmelik, yönerge, prosedürlerinde ve ilgili mevzuatta belirtilen kurallara uymakla sorumludurlar.

### 1.2. Uygunsuz Kullanım

Kullanıcıların, kendilerine sağlanan BT olanaklarını Üniversite ilke ve hedefleri doğrultusunda görevleri gereği kullanması beklenmektedir. Kullanıcıların yetkileri oranında olanaklardan faydalanma şekli gözetim ve denetim altına alınmamış olmakla birlikte kullanıcılar aşağıda bahsedilen uygunsuz kullanımlarının sonuçlarından sorumlu tutulurlar. Uygunsuz Kullanım durumları, oluşumu ve etkisi açısından iki ana grupta ele alınır.

**a) Doğrudan teknoloji altyapısını etkileyen ve ilgilendiren kasti veya sürekli ihmal durumları;** Örneğin virüs yayılmasına neden olmak, güvenlik açıklarından faydalanmak, sabote etmek, erişimi engellemek, izinsiz bilgi kaçırmak, vb.

**b) Üniversite tarafından sağlanan ve işletilen ortam veya olanakları kullanmak suretiyle çeşitli Üniversite kurallarının ve/veya yasaların ihlal edildiği durumlar;** Örneğin e-posta aracılığı ile bir başkasını veya bir kurumu küçük düşürmek, taciz veya hakaret etmek, iletişim ağını kullanarak üçüncü parti bir kurum veya kişiye zarar vermek vb.

### 1.3. Bilgi Teknolojisi Birimi

Üniversite adına BT olanaklarını planlayan, kuran, işletim, destek ve güvenlik hizmetlerini yürüten sorumlu birimdir. İhtiyaç anında (216) 483 9988 nolu telefondan Çağrı Merkezi aracılığı ile BT Birimine ulaşılabilir.

### 1.4. İlgili Yönetmelikler ve Kanunlar

Bu belge içindeki konular ile ilgili olarak başvurulacak, aşağıda sayılanlarla sınırlı olmamak üzere esas Üniversite yönergeleri ve kanunlar şöyledir:

- Bilgi Teknolojisi - Bilgi İşlem Olanaklarının Kullanımı yönergesi
- Bilgi Teknolojisi - Erişim Yönetimi yönergesi
- 5651 sayılı Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun
- 5846 sayılı Fikir ve Sanat Eserleri Kanunu
- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 4857 sayılı İş Kanunu
- 5237 sayılı Türk Ceza Kanunu

## 2. ÜNİVERSİTENİN SORUMLULUKLARI

Üniversite, kullanıcı bilgisayarlarında, sunucu sistemlerinde ve iletişim ağında güvenlik, felaket durumlarına hazırlık ve iş sürekliliği tedbirlerini (antivirüs, yedekleme, güvenlik duvarı vb.) alır ve kullanıcıları çeşitli yollarla bilgilendirir.

Üniversite kendi sorumluluğunda olan iletişim ağı üzerindeki tüm aktiviteleri, resmi makamlarca yapılmış başvurulara istinaden, ilgili mevzuat hükümleri gereğince resmi makamlarla paylaşmakla yükümlüdür. Bu kapsamda, kullanıcıların erişimleri engellenmez ve denetlenmez ancak tüm erişim kayıtları gerektiğinde delil olarak kullanılmak üzere saklanır.

## 3. KULLANICILARIN SORUMLULUKLARI

### 3.1. Kurumsal Bilginin Saklanması ve Gerekli Hallerde Paylaşımı

Üniversite içi bilgi paylaşımı sadece görev gereği ilgili veriye ulaşması gereken çalışanlar arasında olmalıdır. Üniversite'ye ait kurumsal veriler, Dosya Sunucuları, Doküman Yönetim Sistemi, Kurumsal Uygulamalar ve Veritabanları gibi Üniversite tarafından sağlanan ve güvenlik tedbirleri denetlenen sunucu ortamları üzerinde saklanmalıdır. Kurumsal veriler, mümkün olduğu oranda çevrim dışı ortamlarda (DVD, taşınabilir bellek, disk, e-posta, basılı doküman vb.) çoğaltılarak kurum dışına çıkarılmamalıdır. Böylesi bir zorunluluğun ortaya çıkması durumunda, paylaşılan kurumsal veri şifrelenmeli, ilgili medya veya bilgiye üçüncü parti şahısların erişimini engelleyecek her türlü tedbir alınmalı ve sonrasında erişimi engelleyecek şekilde gerekli imha işlemi yapılmalıdır.

Kullanıcılar bilgisayarlarının başında olmadıkları durumda, sadece kullandıklarına tahsis edilmiş bilgilerin ve yetkilerinin üçüncü şahıslar tarafından kullanımını engellemek için gerekli tedbirleri almakla sorumludurlar (örneğin bilgisayar şifresi hiçbir şekilde üçüncü kişilerle paylaşılmamalı, bilgisayarlarda şifre erişimli ekran koruyucu kullanılmalı, mekanlar kilitlenmelidir).

### 3.2. Üniversite Ağına Uzaktan Erişim

Üniversite olanaklarına uzaktan erişim için Üniversite tarafından sağlanan bilgisayarların kullanımı tercih edilmelidir. Genel kullanıma açık bilgisayarlar veya iletişim ağları (İnternet kafe, farklı kurum ağları, ortak kullanılan bilgisayarlar, vb.) üzerinden Üniversite olanaklarına uzaktan erişim, mümkün olduğunca kullanılmamalıdır. Böylesi bir zorunluluk ortaya çıkmışsa, gerçekleştirilen erişimin güvenli olduğundan, kriptolojik şifrelemenin (SSL) kullanıldığından, şifrelerin kayıt edilmediğinden emin olunmalıdır. Herhangi bir şüpheli durum oluşması durumunda derhal Üniversite tarafından verilen şifreler değiştirilmeli ve Bilgi Teknoloji biriminden yardım istenmelidir.

### 3.3. Olanakların Görev Dışı Kullanımı

Olanakların, Üniversite ilke ve hedefleri doğrultusunda kullanımı hedeflenmekle birlikte, iletişim ortamının görev dışı veya sosyal kullanımı engellenmemiş, denetim altına alınmamıştır. Üniversite tarafından bir ayrıcalık olarak tanınan bu özgür ortamın kötüye kullanımı (iş aksatma, verimsizlik, kaynak tüketimi, vb.) durumunda birim yöneticilerinin görüş ve onayı paralelinde tedbirler alınabilir.

Olanakların, kullanıcılar tarafından ticari fayda elde etme amacıyla kullanımına izin verilmez. Böyle bir durumun tespiti halinde ise Üniversite'nin her türlü yasal hakkı saklıdır.

### 3.4. Lisanslı Yazılım, Belge ve Eser Kullanımı

Üniversite lisans hakları ödenmiş standart yazılımlar ile birlikte kullanıcılara bilgisayar sağlamaktadır. Kullanıcılar bilgisayarlarına ek olarak yükleyecekleri yazılımların lisans şartlarını yerine getirmekten ve yükümlülüklerin yerine getirilmemesi halinde olası yasal sonuçlarından (adli para cezası ve hapis cezası gibi) şahsen sorumludurlar.

Üniversite telif hakları kanunları ile korunan birçok lisanslı yazılım, bilgi, belge ve eseri iletişim ağı üzerinden kullanıcıların erişimine açmaktadır. Kullanıcılar söz konusu lisans şartlarını yerine getirmelidir. Üniversite sağladığı bilgisayar veya ortam nedeniyle, suç sayılabilecek davranışlar neticesinde kullanıcılar adına yasalar karşısında sorumlu değildir.

Üniversite, kullanıcıların internet üzerinden bilgisayarlarına kopyaladıkları veya dağıttıkları, telif hakları ile korunan her türlü bilgi, belge, film, müzik vb.'den kaynaklanabilecek sorunlardan dolayı iletişim ortamını sağladığı için sorumlu tutulamaz. Söz konusu içeriğin yasal sorunlara neden olması durumunda Üniversite ilgili mevzuat gereğince kullanıcılar hakkındaki bilgileri yasal mercilere verecektir.

### 3.5. Sabotaj, Bilgi Kaçırma, Yetkisiz İşlem, İhmal

Üniversite, bilgi sistemlerine, diğer kullanıcı ve kurumsal bilgilere dönük her türlü kasti davranış veya ihmal sonucu ortaya çıkan zarar (bilgi silme, kaçırma, yanıltma vs.) karşısında, önleyici teknik tedbirleri alma, yasal takip başlatarak varsa zararı veya itibarı tazmin yoluna gitme hakkına sahiptir. Yasal takip çerçevesinde kullanılmak üzere Üniversite'ye ait sistemlerdeki erişim kayıtları delil kabul edilir.

### 3.6. Konfigürasyon ve Güvenlik Tanımları

Kullanıcılar teknik olarak mümkün olsa bile, standart yazılımlar ve orijinal ayarları ile teslim edilen bilgisayarlardaki güvenlik düzeyini düşürmemelidir. Güvenlik ayarlarına örnek olarak; MS Internet Explorer ve MS Outlook'u etkileyen güvenlik alanları ayarları (Internet Explorer security zone settings), virüs koruma program ayarları, işletim sistemi güncelleme ayarları, kişisel koruma duvarı ayarları, BIOS ayarları ve diğer donanımsal ve yazılım güvenlik ayarları sayılabilir.

Üniversite tarafından sağlanan bilgisayarlara, kurumsal ve kişisel verilere erişimi kolaylaştırıcı, güvenlik zafiyetleri içeren yazılımlar kurulmamalı ve kullanılmamalıdır (örn. torrent yazılımları, sistematik dosya indirme, paylaşma yazılımları vb.).

### 3.7. Güvenlik Olay ve Zayıflıklarının Bildirimi

Kullanıcıların, güvenlik olaylarına ve zayıflıklarına karşı duyarlı davranmaları beklenir. Kullanıcılar, fark edilen her türlü güvenlik zayıflığını, kontrollerindeki kritik kurumsal bilgi, belge ve ilgili ekipmanların kaybı veya çalınması durumunu en kısa zamanda Üniversite Bilgi Teknolojisi birimine bildirmekle yükümlüdür..

## 4. UYGUNSUZ KULLANIM DURUMLARININ ÇÖZÜMLENMESİ

Doğrudan Üniversite BT olanaklarını hedef alan uygunsuz kullanım durumlarında (saldırı, servisi durdurma, bilgi kaçırma vb.) BT birimi tarafından sorunu acilen ortadan kaldırıcı teknik çalışma gerçekleştirilir. Böylesi durumlar, gerekli araştırma faaliyetleri yapıldıktan sonra, ilgili kullanıcının erişiminin engellenmesi ile sonuçlanabilir. Olayın sonuçlarına bağlı olarak ilgili kullanıcı uyarılır ve/veya zararı tazmin etmek, tekrarını önlemek adına Üniversite yönetmelik, yönerge ve ilgili mevzuata uygun olarak işlem yapılır.

Üniversite BT olanakları kullanılarak ortaya çıkan, genellikle içerik kaynaklı uygunsuz kullanım durumlarında ise resmi makamlarca yapılan başvurulara istinaden delil teşkil eden erişim kayıtları ilgili mevzuat gereğince ilgili makamlara teslim edilir.

Yukarıdaki metni okudum ve anladım.

Ad Soyad

İmza

Tarih