# AMAÇ

Bu talimat ile kurumsal bilgi güvenliğinin en yüksek seviyede sağlanması, bilgi varlıklarının korunabilmesi kurumun karşılaşabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması, kurumsal bilgi güvenliği bilincinin geliştirilmesi amaçlanmıştır.

# KAPSAM

Bu talimat bilgi güvenliğinin sağlanması ile ilgili işlemleri kapar.

# TANIMLAR

# SORUMLULAR:

## Bilgisayar kullanıcıları

## Bilgi İşlem Birimi Görevlisi

# İLGİLİ DOKÜMANLAR

# UYGULAMA

## **Genel Kullanım Kuralları**

Bilişim ile alakalı sistemler (bilgisayar, yazılım, işletim sistemleri, kayıt cihazları, e-mail, www, ftp vs.) Kurumun sahip olduğu değerlerdir. Bu sistemler kamuya hizmet için kullanılmalıdır. Güçlü bir güvenlik bütün çalışanların içerisine dahil olduğu takım çalışmasıyla oluşturulabilir. Bütün bilgisayar kullanıcıları günlük aktivitelerini yerine getirebilmesi için bu kuralları iyi bilmeli ve uygulamanın sorumluluğunu taşımalıdır.Bu madde altındaki faaliyetlerden kullanıcılar sorumludur.

* Kullanıcılar şunun farkında olmalıdırlar; kurumun güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da Kurumun bünyesinde oluşturulan tüm veriler Kurumunun mülkiyetindedir.
* Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.
* Bilgisayarlar üzerinden resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamamalıdır.
* Kurumda Bilgi İşlem Biriminin bilgisi olmadan Fakülte Ağ sisteminde (web hosting servisi, e-posta servisi vb.) sunucu nitelikli bilgisayar bulundurulmamalıdır.
* Birimlerde sorumlu Bilgi İşlem Personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları .kaynak profilleri v.b. üzerinde mevcut yapılan düzenlemelerin hiçbir surette değiştirilmemelidir.
* Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

## **Güvenlik ve Kişiye Ait Bilgiler**

* Şifreleri güvenli bir şekilde tutun ve hesabınızı başka kimselerle paylaşmayın. Sistem seviyeli şifreler üç ayda bir kullanıcı seviyeli şifreler ise en az altı ayda bir değiştirilmelidir. Kullanıcı, şifresini başkası ile paylaşmamalı, kağıtlara yada elektronik ortamlara yazmamalıdır.
* Bir kullanıcı adı ve şifresinin birim zamanda birden çok bilgisayarda kullanılmamalıdır. Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.
* Laptop bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda Bilgi İşlem Birimine haber verilmelidir.Çalışanlar bilinmeyen kimselerden gelen dosyaları açarken çok dikkatli olmalıdırlar. Çünkü bu mailler virüs, e-mail bombaları ve Truva atı gibi zararlı kodlan içerebilirler.
* Bütün kullanıcılar ağın kaynaklarının verimli kullanımı konusunda dikkatli olmalıdırlar. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olun ve gerekirse dosyaları sıkıştırın.
* Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan (örnek, elektronik bankacılık vs.) sistemin sahibi sorumludur.
* Bilinmeyen kaynaklardan gelen USB bellek ve Cd-Rom’ları daima virüslere karşı tarama yapın.

## **Uygunsuz Kullanım**

**Aşağıdaki aktiviteler hiçbir istisna olmadan kesinlikle yasaklanmıştır.**

* Herhangi bir kişi veya kurumun izinsiz kopyalama, ticari sır, patent veya diğer şirket bilgileri, yazılım lisanları vs haklarını çiğnemek.
* Kitapların izinsiz kopyalanması, magazinlerdeki fotoğrafların dijital formata dönüştürülmesi, lisans gerektiren yazılımların kopyalanması.
* Zararlı programların (örnek, virüs, solucan, truva atı, e-mail bombaları vs) ağa veya sunuculara bulaştırılması.
* Kendi hesabınızın şifresini başkalarına vermek veya kendi hesabınızı kullandırmak. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışmak.
* Ağ güvenliğini etkilemek (örnek, bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ haberleşmesini bozmak (paket sniffing, paket spoofing, denial of service vs.).
* Port veya ağ taraması yapmak.
* Kullanıcı kimlik tanıma yöntemlerinden kaçmak.
* Program/scrIPt/ komut kullanarak kullanıcının bağlantısını etkilemek.
* Kurum bilgilerini kurum dışından üçüncü şahıslara iletmek.
* Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Birimi onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapması.
* Cihaz, yazılım ve verinin izinsiz olarak kurum dışına çıkarılması.
* Kurumun politikaları olarak belirlediği programlar dışında kaynağı belirsiz olan programları (Dergi CD’leri veya internetten indirilen programlar vs) kurmak ve kullanmak yasaktır.

## **E-posta**

* Kurumun e-posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz. Bu tür özelliklere sahip bir mesaj alındığında hemen ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.
* Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
* Fakülte ile ilgili olan hiçbir gizli bilgi, gönderilen mesajlarda yer alamaz. Bunun kapsamına içerisine iliştirilen öğelerde dahildir.
* Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e- postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
* Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
* Kişisel kullanım için Internet’teki listelere üye olunması durumunda kurum e- posta adresleri kullanılmamalıdır.
* Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e- posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
* Çalışanlar e-posta ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme, vb) gönderemezler.
* Kişisel amaçlar için e-posta kullanımı mümkün olduğunca makul seviyede olmalıdır. Ayrıca iş dışındaki e-postalar farklı bir klasör içerisinde saklanmalıdır.
* Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-maillerin sahte e-mail olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın derhal silinmelidir.
* Kurum çalışanları mesajlarını düzenli olarak kontrol etmeli ve kurumsal mesajları cevaplandırmalıdır.
* Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
* Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.
* Elektronik postaların sık sık gözden geçirilmeli, gelen mesajların uzun süreli olarak genel elektronik posta sunucusunda bırakılmamalı ve bilgisayardaki kişisel klasör’a (personel folder) çekilmelidir.
* E-posta adresine sahip kullanıcı herhangi bir sebepten birim değiştirme, emekli olma işten ayrılma sebepleriyle kurumdaki değişikliğinin yetkililer tarafından Rektörlük Bilgi İşlem Merkezine bu değişikliği en geç 15 gün içinde bildirmelidir.
* Çoğu internet servis sağlayıcısı ve e-posta sağlayıcısı spam filtresi sunar. Ancak kurduğunuz seviyeye bağlı olarak istediğiniz postaları engellemeyle de sonuçlanabilirsiniz. Filtrenin istediğiniz şekilde çalıştığından emin olmak için arada sırada önemsiz postalarınızı kontrol etmekte fayda olabilir.
* Çoğu e-posta sağlayıcısı e-postayı spam olarak işaretlemenin veya spam örneklerini ihbar etmenin yollarını sunmaktadır. Spam’i ihbar etmek aynı zamanda o mesajın doğrudan gelen kutusuna düşmesini de engeller.
* E-posta adresinizi internet ortamındaki özellikle sosyal ağ profillerinizde saklamadığınıza veya kişisel bilgilerinizi sadece belirli kişilerle paylaşıldığından emin olunmalı. İnternet ortamındaki bazı mecbur kalınan ve e-posta adresini vermek istemediğiniz yerlerde anlık e-posta servislerini kullanınız.
* E-posta iletilerindeki, metin mesajlarındaki, pop-up pencerelerindeki veya anlık mesajlardaki linklere tıkladığınız takdirde açılan sayfaya dikkat edin. Doğrudan linklere tıklamak yerine, linki adres çubuğuna kopyalayıp sayfayı açmayı denemeyi alışkanlık edininiz.
* Sık kullandığınız ve bankacılık işlemleri gibi kritik kullandığınız web sayfalara arama motoru veya adres çubuğundan ulaşmak yerine web tarayıcılarınızda sık kullanılanlar oluşturarak ulaşınız.
* Banka hesap veya kredi kartı ekstrenizi düzenli olarak kontrol ediniz. Sizin bilginiz dışında yapılmış işlemlerle ilgili olarak gereken işlemleri yapınız.
* Herkese açık kablosuz ağ noktalarını kullanarak veya herkese açık bir bilgisayardan hiçbir zaman bankacılık ve benzeri kritik işlemlerinizi gerçekleştirmeyiniz. Eğer herkese açık bir bilgisayardan giriş yapacaksanız, bilgisayarın şifre korumalı olmasına özen gösteriniz.

## **Web Güvenliği**

İnternet sitelerinde gezinti yaparken bilgisayarımıza virüs ve tehlikeli yazılım bulaştırma ihtimali yüksek olan siteler genellikle şunlardır;

* Çok fazla bilinmeyen siteler
* Bahis siteleri
* Pornografik siteler
* Korsan yazılım indirilen siteler
* Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek,
* E-posta mesajları ile gönderilen bağlantılara dikkat etmek,

## **Bilgi Güvenliği Faaliyetleri**

Bu madde altındaki faaliyetlerden Bilgi İşlem Birimi Görevlileri sorumludur.

* Üniversitesi Diş Fakültesi ağına bağlı bütün bilgisayarlar düzenli olarak güncel anti-virus yazılımı ile taranmalıdır.
* Buna ek olarak anti-virus yazılımı ve virüs patternleri otomatik olarak güncellenmelidir. Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır.
* 6284 Sayılı Yasanın 8/6 nolu Maddesi uyarınca, kimlik bilgileri veya kimliği ortaya çıkarabilecek bilgilerin gizli tutulması gereken hastaların kimlik bilgileri veya kimliği ortaya çıkarabilecek bilgilerinin otomasyon sisteminde gizliliği korunmalıdır.