

# TOROS ÜNİVERSİTESİ BİLGİ VE İLETİŞİM GÜVENLİĞİ USUL VE ESASLARI

## BİRİNCİ BÖLÜM

### Amaç, Kapsam, Dayanak ve Tanımlar

#### Amaç

**Madde 1 -** (1) Bu Esasların amacı, Toros Üniversitesinde bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilginin/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetler ile Toros Üniversitesi nezdinde işlenen kişisel veri niteliğindeki verilerin korunması için bilgi güvenliği kapsamında uyulması gereken usul ve esasların e ilişkin usul ve esasları düzenlemektir.

#### Kapsam

**Madde 2 -** (1) Bu Esaslar, Toros Üniversitesi personeli ve öğrencileri ile kendilerine herhangi bir nedenle geçici veya kalıcı veya kısıtlı olarak Toros Üniversitesi Bilişim Kaynaklarını kullanma, yönetme veya izleme olanağı sunulan kişileri, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini, hizmet sağlayıcılarını, sistem, veri ve bilgi kullanıcılarını ve Üniversite bilgi işlem altyapısını kullanmakta olan tüm birimleri kapsar.

#### Dayanak

**Madde 3 -** (1) Bu Esaslar, 4/11/1981 tarihli ve 2547 sayılı Yükseköğretim Kanununun 14'üncü maddesi, 6698 Sayılı Kişisel Verilerin Korunması Kanunu, 6 Temmuz 2019 tarihli ve 30823 Sayılı Resmî Gazetede yayımlanan 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi ile 10.07.2020 tarihli T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberine dayanılarak hazırlanmıştır.

#### Tanımlar ve Kısaltmalar

**Madde 4 -** (1) Bu Esaslarda geçen;

- Başkan: Toros Üniversitesi Bilgi ve İletişim Güvenliği Komisyonu Başkanı,
- Komisyon: Toros Üniversitesi Bilgi ve İletişim Güvenliği Komisyonu'nu,
- Rektör: Toros Üniversitesi Rektörü'nü,
- Senato: Toros Üniversitesi Senatosu'nu,
- Üniversite: Toros Üniversitesi'ni
- BİDB: Bilgi İşlem Daire Başkanlığını ifade eder.

## İKİNCİ BÖLÜM

### Bilgi ve İletişim Güvenliği Komisyonunun Oluşturulması, Bilgi Güvenliği Hedefleri

#### Bilgi ve İletişim Güvenliği Komisyonunun Oluşumu ve Çalışma Esasları

**Madde 5 -** (1) Bu Esaslarda belirtilen hedefleri ve uygulamaları yürütmek, çalışmalarının etkin ve verimli bir şekilde yürütülmesini sağlamak üzere Rektör tarafından Bilgi ve İletişim Güvenliği Komisyonu oluşturulur. Komisyon bir Rektör Yardımcısı başkanlığında, Üniversite Kalite Koordinatörü, Uzaktan Eğitim Merkezi Müdürü, Genel Sekreter, Bilgi İşlem Daire Başkanı, Hukuk Müşaviri, Öğrenci İşleri Daire Başkanı, İnsan Kaynakları Daire Başkanı, Kurumsal İletişim Müdürü ve bilgisayar ve yazılım alanında bir öğretim elemanından oluşur. Komisyonun raportörlüğü, alınan

kararların Rektörlüğe iletmesi ve Komisyonun görev alanına giren konularda yürütülecek idari işlemlerin sekreteryası BİDB tarafından yürütülür.

(2) Komisyon, Başkanın belirleyeceği tarihlerde, Başkanın çağrısı üzerine en az yılda 1 kez toplanır. Başkan veya üyeler belirli dönemler dışında da toplantı isteyebilir. Bilgi ve İletişim Güvenliği Komisyonu, üye tam sayısının salt çoğunluğuyla toplanır ve toplantıya katılanların salt çoğunluğuyla karar alır. Oyların eşit olması durumunda Komisyon Başkanının oyu yönünde karar alınmış sayılır.

### **Komisyonun Görevleri**

**Madde 6 -** (1) Komisyonun görev, yetki ve sorumlulukları şunlardır:

a) Üniversitenin Bilgi ve İletişim Güvenliği Sistemini oluşturmak ve sürdürülebilirliğini sağlamak,

b) Bilgi ve İletişim Güvenliği Sistemi uygulamalarının bu Esaslara uygun olarak yürütülmesini sağlamak,

c) Üniversite Bilgi ve İletişim Güvenliği Sisteminin birimler düzeyinde kurulması, sürdürülmesi ve iyileştirilmesi için gerekli koordinasyonu sağlamak ve öneriler geliştirmek,

ç) Gerekli görülen durumlarda Komisyon bünyesinde alt ekipler oluşturmak, çalışma usul ve esaslarını belirlemek,

d) Bilgi ve İletişim Güvenliği Sisteminin uygulanmasında katılımcılığa, kaynakları etkin ve verimli kullanmaya, süreçleri iyileştirmeye dayalı bir kurum kültürünün geliştirilmesini ve yaygınlaştırılmasını sağlamak,

e) Bilgi ve İletişim Güvenliği Sisteminin etkinliğini artırıcı politikalar belirlemek ve uygulamaya yönelik kararlar almak,

f) Bilgi ve İletişim Güvenliği Sistemi kapsamında yapılan inceleme, araştırma, denetim faaliyetleri sonucunda tespit edilen bulgulara ilişkin düzeltici/iyileştirici kararları almak; uygulamalara ilişkin değerlendirmelerde bulunmak, bilgi ve iletişim güvenliği denetiminin planlandığı şekilde yapılması için gerekli kaynakları sağlamaktır.

### **Bilgi Güvenliği Hedefleri**

**Madde 7 -** (1) Bilgi güvenliği, Üniversitedeki işlerin sürekliliğinin sağlanması, Üniversitenin faaliyetlerinde meydana gelebilecek aksaklıkların engellenmesi veya azaltılması ve bilginin geniş çaplı tehditlerden korunmasını sağlar. Bilgi güvenliği temelde aşağıdaki üç unsuru hedefler.

a) Gizlilik: Bilginin yetkisiz kişilerin erişimine kapalı olması şeklinde tanımlanmakta olup, başka bir deyişle bilgiye yetkisiz kişilerce ulaşılmasını veya bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesini hedefler.

b) Bütünlük: Bilginin, kasten veya ihmal ile yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı, bilginin içeriğinin korunarak bozulmamış olmasını hedefler.

c) Kullanılabilirlik: Bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olmasını hedefler. Bu unsur, herhangi bir sorun halinde bile bilginin erişilebilir olmasını gerektirmekte olup, bu erişim, kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesine göre, her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

ç) Üniversite yönetimi, Üniversite'nin iş faaliyetlerinin en az kesinti ile devam etmesini ve kişisel verilerin hukuka uygun işlenmesini sağlamak ve herhangi bir kişisel veri ihlalini önlemek için bilgi işlem hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziki ve dijital verilerin bilgi güvenliğini sağlamayı hedefler.

## ÜÇÜNCÜ BÖLÜM

### Bilgi ve İletişim Güvenliği Uygulamalar ve Önlemleri

#### Uygulamalar

**Madde 8 -** (1) Komisyon, Üniversitenin Bilgi ve İletişim Güvenliği hedefleri doğrultusunda bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlemek amacıyla hangi yazılım ve servislerin çalıştığını; güvenlik yazılımı mesajları, erişim kontrolü kayıtları ile diğer raporlama araçlarını düzenli olarak kontrol eder. Zafiyet taramaları ve sızma testlerinin yapılması sonucu ortaya çıkan güvenlik açıklarına dair testlerin sonuçlarını değerlendirerek gerekli idari ve teknik önlemleri alır. İstenmeyen olaylar yaşanması durumunda Üniversite, söz konusu olay hakkındaki delilleri toplayarak güvenli bir şekilde saklanmasını sağlar.

(2) Üniversite, yukarıdaki teknik ve idari tedbirler kapsamında çalışanlar ve öğrencilerin uyması için standartlar ve kurallar belirlemekte olup bunlar aşağıdaki gibidir.

#### a) E-Posta Kullanma Kuralları

1. Üniversite'nin elektronik posta sistemi, kullanıcının şahsi sosyal medya (facebook, twitter, instagram vb.) hesapları ve/veya herhangi bir kişisel uygulama için ve/veya kişisel amaçlar ile kullanılamaz.

2. Kötü amaçlı, spam, sahte vs. nitelikteki zararlı elektronik postalara yanıt yazılmamalı, bu elektronik postalara iliştilmiş her türlü çalıştırılabilir dosya içeren elektronik postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.

3. Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen elektronik postaların sahte elektronik posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın işbu elektronik postalar derhal silinmelidir.

4. Çalışanlar ve öğrenciler, Üniversite'nin elektronik posta sistemi aracılığıyla uygun olmayan içerikleri (pornografî, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.

5. Çalışanlar ve öğrenciler, elektronik posta ileti ve her türlü mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidirler. Elektronik posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.

6. Üniversite çalışanları ve öğrenciler, kurumsal elektronik postaların Üniversite dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

7. Kaynağı bilinmeyen elektronik posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmeli olup, bu şekilde gelen elektronik postalar BİDB'na bildirilmelidir.

8. Kullanıcılar kendilerine ait elektronik posta adresinin şifresinin güvenliğinden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren Üniversite'nin BİDB ve Komisyon ile temasa geçip onlara durumu haber vermekle yükümlüdürler.

9. Üniversite'den ayrılan personel, kurumsal elektronik posta sistemini kullanmaya devam edemez. Elektronik posta adresine sahip kullanıcının birim değiştirme, işten ayrılma gibi herhangi bir sebeple önceden çalışmakta olduğu birim veya Üniversite ile ilişkisinin sona ermesi durumunda elektronik posta sisteminde gerekli değişiklikler yetkililer tarafından BİDB'na en kısa zamanda bildirilir ve yapılan bildirim üzerine ilgili hesap silinir, yok edilir veya ilgili personelin hesaba erişimi engellenerek yalnızca yetkili kişilerin ulaşacağı şekilde arşivlenir.

#### b) İnternet Kullanım Politikası

1. Hiçbir kullanıcı, Üniversite'nin tavsiye ettiği veri paylaşım yöntemi dışındaki bir veri paylaşım kanalını kullanamaz. (Örneğin; Bittorent, iMesh, eDonkey, Aimster vb. peer-to-peer bağlantı yollarını içeren programlar kullanılamaz.)

2. Üniversite faaliyetleri kapsamında farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecek olması durumunda çalışanlar, bağlantılarının SSL ya da BİDB tarafından belirlenecek olan daha güvenli bir yol ile gerçekleştirilmesinden sorumludur.

3. Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde mesajlaşma ve sohbet programları gibi mesajlaşma programları kullanılamaz.

4. Hiçbir kullanıcı özel amaçlı olarak internet üzerinden Multimedia Streaming (Video, müzik ve iletişim vb. için) yapamaz.

5. Üniversite kapsamında yürütülen faaliyetler ile ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyalar göndermek, (upload) indirmek (download) veya böylesi dosyaları bilgisayarlarda saklamak yasaktır. Buna ek olarak, iş ile ilgisi olmayan ve kişilere ait görsel ve işitsel içerikler Üniversite'nin veri depolama sistemlerine aktarılamaz, bu sistemlere kaydedilemez veya bu sistemlerde tutulamaz. Böyle bir işlem, kişinin kendisi sorumlu olacak olup herhangi bir kişisel veri ihlalinde Üniversite sorumlu tutulamayacaktır.

6. İnternet üzerinden Üniversite'nin BİDB tarafından onaylanmamış yazılımlar indirilemez ve Üniversite sistemleri üzerine bu yazılımlar kurulamaz, kullanılamaz.

7. Üniversite ağlarından ve bilgisayarlarından genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.

8. BİDB, iş kaybının önlenmesi için çalışan ve öğrencilerin internet kullanımı hakkında gözlem yapabilir ve bu konuda istatistiksel amaçlarla kullanıcıların işlem hareketlerinin kaydını tutabilir. Gerekli durumlarda internet üzerinde kısıtlamalar yapabilir, çalışan ve öğrencilere uyarıda bulunabilir.

9. Üniversite'ye ilişkin sistemler üzerinden herhangi bir siyasi içerik ya da propaganda paylaşımı yapılamaz.

#### c) Genel Kullanım Politikası

1. Bilgisayar başından uzun süreli uzak kalınması durumunda bilgisayar kilitlenmeli ve 3. şahısların bilgi ve kişisel verilere erişimi engellenmelidir. Bilgisayarların, kullanılmama halinde, kilit ekranına geçiş süresi [5] dakika olup, bu sürenin sonunda bilgisayarlar kendiliğinden uyku moduna geçecektir.

2. Üniversite verilerini içeren bir bilgisayarın veya taşıyıcının çalınması, kaybolması gibi durumlarda, bu durum derhal ve herhalde en geç [24] saat içinde BİDB'na ve Komisyon'a bildirilmelidir.

3. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek Üniversite'ye veya kişiye yönelik, elektronik bankacılık, hakaret veya siyasi içerikli mail, kullanıcı bilgileri ve bunun gibi saldırılardan kullanıcı sorumlu olacaktır.

4. Üniversite bilgisayarları aracılığıyla yasadışı olaylara karışılmamalıdır.

5. Bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi gibi ağ güvenliğini veya ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişilmemelidir.

6. Üniversite bilgileri ve bunun kapsayabileceği kişisel veriler, yetkili kişiler dışında ve ilgili kişinin açık onayı olmaksızın üçüncü kişilere aktarılmamalıdır.

7. Kullanıcıların kişisel bilgisayarları üzerine BİDB'nin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

8. Herhangi bir cihaz, yazılım veya veri, Üniversite'nin faaliyetleri kapsamında gerekli olmadığı sürece izinsiz olarak Üniversite dışına çıkarılmamalıdır. [Gerekli olduğu takdirde ise, [BİDB] bu hususta bilgilendirilecektir.]

9. Üniversite'nin kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları kullanmak yasaktır.

10. BİDB, yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığını düzenli olarak kontrol eder ve kullanılmayan yazılım ile servislerin silinmesini sağlar. Üniversite tarafından yasaklanmış veya herhangi bir sebeple silinerek kullanımdan kaldırılmış yazılım, donanım ve/veya servislerin çalışan ve öğrenciler tarafından Üniversite bilgisayarları üzerinden kullanılması yasaktır.

11. Çalışan ve öğrenciler, kendilerine tahsis edilen ve Üniversite çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki gerek Kurumsal gerek kişisel verilerin güvenliğinden sorumludur. Bu doğrultuda, çalışanlar ve öğrenciler Üniversite'nin uygulamaya koyduğu politika, yönerge ve talimatlar doğrultusunda gerekli fiziki ve teknik önlemleri alır ve uygular.

12. BİDB kullanıcıya haber vermeksizin, Üniversite'nin faaliyetlerinin ve verilerinin güvenliğini sağlamak amacıyla, yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir, gereken teknik veya idari tedbirleri uygulayabilir.

13. Üniversite tarafından çalışanlara tahsis edilen cihazlarda ve bilgisayarlarda oyun ve eğlence amaçlı programlar kullanılamaz, çalıştırılmaz ve bu tarz program ve uygulamalar Üniversite bilgisayarlarına kopyalanamaz.

14. Bilgisayarlar üzerinden Üniversite'nin faaliyetleri kapsamında gerekli olanlar haricinde dosya alışverişinde bulunulmamalıdır.

15. Üniversite'de BİDB'nin bilgisi olmadan ağ sisteminde (Web Hosting, E- Posta Servisi vb.) sunucu niteliğinde olan bilgisayar ve cihaz bulundurulmamalıdır.

16. BİDB'nin bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

17. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisanssız yazılımı Üniversite tarafından kendisine tahsis edilen bilgisayarında barındıran çalışan veya Üniversite bilgisayarını kullanan öğrenci veya çalışan, bu durumdan kendisi sorumlu tutulacaktır.

18. Gereksizlikçe bilgisayar kaynakları paylaşımına açılmamalıdır, kaynakların paylaşımına açılması halinde mutlaka şifre kullanım kurallarına göre hareket edilmelidir.

19. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, problem hakkında ivedilikle BİDB'ye ve Komisyon'a haber verilmelidir.

#### ç) Antivirüs Politikası

1. Antivirüs yazılımı yüklü olmayan bilgisayar, ağa bağlanmamalı ve hemen BİDB'ye konu ile ilgili olarak haber verilmelidir.

2. Zararlı programları (virüsler, solucanlar, truva atı, e-posta bombaları vb.) Üniversite bünyesinde oluşturmak ve dağıtmak yasaktır.

3. Hiçbir kullanıcı, herhangi bir sebepten dolayı Üniversite tarafından kurulumu yapılmış olan antivirüs programını sistemden kaldıramaz ve bilgisayara başka bir antivirüs yazılımını kuramaz.

4. Antivirüs yazılımlarını her daim güncel tutulacak olup, kullanıcıların söz konusu yazılımların güncelliğini etkileyecek işlemlerde bulunması yasaktır.

### **Şifreleme**

**Madde 9 -** (1) Şifreleme, bilgisayar ve her türlü veri kayıt cihazı güvenliği için önemli bir özellik olup, kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar aşağıda belirtilmiştir.

#### **a) Şifre Kullanma Kuralları**

1. Uluslararası kabul gören şifreleme programları kullanılmalıdır.
2. Kullanılan şifreler, kolayca kırılmayacak güce sahip olmalıdır.
3. Şifreler (elektronik posta ve bilgisayar veya veri kayıt cihazına giriş için kullanılan her türlü şifre) en az [6] ayda bir değiştirilmelidir.
4. Şifreler elektronik posta iletilerine veya herhangi bir elektronik forma yazılmamalı ve eklenmemeli, başkası ile paylaşılmamalı, fiziki ya da elektronik ortamlara yazılmamalıdır.
5. Herhangi bir kişiye telefonda veya herhangi bir iletişim aracıyla şifre verilmemelidir.
6. Şifreler, işten uzakta olunan zamanlarda dahi iş arkadaşlarıyla paylaşılmamalıdır.
7. Şifre [3] defa üst üste yanlış girildiğinde bilgisayar kilitlenmelidir.
8. Çoklu giriş yapılan bilgisayarlara giren personellere şifre kullanımı ve kişisel veri güvenliği hakkında uyarılar yapılmalıdır.
9. Mutlaka ekran kilidi kullanılmalı ve ekranın [5] dakika hareketsiz kalması halinde ekran kilidi devreye girmelidir.
10. Üniversite bünyesinde kullanılan şifreler Üniversite dışında (bankacılık işlemleri vb.) herhangi bir şekilde kullanılmamalıdır.
11. Değişik sistemler için farklı şifreleme kullanılmalıdır (örneğin, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanılmalıdır).
12. Herhangi bir kimse şifre isteğinde bulunursa, kişi işbu Yönerge referans gösterilerek BİDB ile Kişisel Verilerin Korunması Komisyonu'na yönlendirilmelidir.
13. Uygulamalarda ve browserlardaki "şifre hatırlama" özellikleri seçilmemelidir.

#### **b) Şifre Oluşturma Kuralları**

1. Şifre; küçük ve büyük karakterler (a-z, A-Z) ile rakam ve semboller (0-9, !'^+%&/()=?\_;\* gibi) içermelidir.
2. Şifre en az sekiz karakterden oluşmalıdır.
3. Şifre oluşturulurken kolayca tahmin edilebilecek kombinasyonlardan kaçınılmalıdır.
4. Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıdan şifresini değiştirmesi talep edilir.

#### **c) Yasak İşlemler**

1. Herhangi bir kişiye telefonda şifre vermek.
2. Elektronik posta mesajlarında şifre belirtmek.

3. Üst yöneticiler ile şifre paylaşmak.
4. Başkaları önünde şifreler hakkında konuşmak.
5. Aile isimlerini şifre olarak kullanmak.
6. Herhangi bir form üzerinde şifre belirtmek.
7. Şifreleri aile bireyleri ile paylaşmak.
8. Şifreleri işten uzakta olunan zamanlarda iş arkadaşlarına bildirmek.

ç) Uygulama Geliştirme Standartları

1. Uygulama geliştiricileri programları, veri bütünlüğünü bozma riskini minimize edecek nitelikte olup bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.

2. Uygulama geliştiricileri programları, şifreleri 'text' olarak veya kolay anlaşılabilir formda saklamamalıdır.

3. Uygulama geliştiricileri programlarının girdilerinin doğruluk ve uygunluk denetimini sağlamak amacıyla kontrol mekanizması yerleştirilmelidir.

4. Uygulama geliştiricileri programları ile kural yönetim sistemi desteklenmelidir. Örneğin; bir kullanıcı diğer bir kimsenin şifresini bilmeden fonksiyonlarına devam edebilmelidir.

d) Uzaktan Erişim ve Aktarım

1. Üniversite'nin bilgisayar ağına uzaktan erişimi tek yönlü şifreleme algoritması veya güçlü şifrelerle yapılmalıdır.

2. Uzaktan erişim için iki kademeli kimlik doğrulama kontrolü uygulanmalıdır.

3. Üniversite'nin bilgisayar ağ bakım onarım gibi teknik sebeplerle uzaktan erişime veya dışarıdan personel erişimine açılacağı zaman kişisel veri koruma önlemleri alınmalıdır. Bu kapsamda kişisel veri içeren dokümanlar şifrelenerek bu dosyalara yetkisiz kişilerin erişimi engellenmelidir.

4. Bakım onarım gibi sebeplerle kişisel veri içeren cihazların üçüncü kişilere gönderilecek olması durumunda cihazlardaki veri saklama ortamları sökülerek güvenli bir yerde saklanmalıdır.

5. Üniversite faaliyetleri kapsamında üçüncü kişilere aktarılacak kişisel veriler, dikkatli bir şekilde ve Üniversite'nin belirleyeceği gerekli tedbirler alınarak gönderilmelidir.

**Yedekleme ve Bulutta Depolama**

**Madde 10 -** (1) Üniversite, çalışan ve öğrencilerin Üniversite faaliyetleri kapsamında kullandığı elektronik cihazlardaki verileri kötü amaçlı yazılımlara karşı yedeklemekte olup, herhangi bir şekilde bir veri kaybı durumunda yedeklenen veriler faaliyete geçirilecektir.

(2) Yedeklenen verilere yalnızca sistem yöneticilerinin erişim yetkisi olup, yetkisiz kişilerce yedeklenmiş verilere erişilmesi yasaktır.

(3) Kişisel veri içeren fiziksel ortamdaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazlar ek güvenlik önlemlerinin olduğu başka bir odaya alınmalı, kullanılmadığı zaman kilit altında tutulmalı ve kullanım halinde oda giriş çıkış kayıtları tutulmalıdır. Bu fiziksel güvenlik önlemlerine ek olarak yedeklenen elektronik ortam ve cihazlardaki veri setler, ağ dışında muhafaza edilerek yedeklenen verilerin siber güvenliği de sağlanmaktadır.

(4) Bulutta depolanan kişisel verilerin içeriği detaylıca belirlenmeli, senkronizasyonu sağlanmalı ve bu veriler, kriptografik yöntemlerle şifrelenerek güvenli bir ortamda yedeklenmelidir.

(5) Bulut bilişim hizmet ilişkisi sona erdiğinde; bulutta depolanan kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarları ve bunların tüm kopyaları yok edilmelidir.

(6) **(Değişik: SNT-05/12/2024-10/52)** Uzaktan Eğitim Sisteminde var olan kaydedilmiş 2 (iki) yıldan önceki tarihli ders dokümanları, sınav evrakları ve ders videoları ilgili akademik dönem sonunda silinebilir.

### **Kişisel Veri İçeren Ortamların Güvenliği**

**Madde 11** - (1) Üniversite yerleşkesi içinde ve dışında yer alan ve Üniversite bünyesinde kişisel veri içeren fiziksel ortamlar (kâğıt vb.) için fiziksel güvenlik önlemleri alınmalı, elektronik ortam ve cihazlar için ise ağ bileşenleri arasında erişimin sınırlandırılması veya bileşenlerin ayrılması yoluyla kişisel verilerin güvenliği sağlanmalıdır. Fiziksel güvenlik önlemleri, Üniversite'nin Dosya ve Arşiv Talimatı, Kişisel Verilerin Korunması ve İşlenmesi Politikası, Özel Nitelikli Kişisel Verilerin Korunması ve İşlenmesi Politikası ve Kişisel Verileri Saklama ve İmha Politikasında belirtilmektedir.

### **Sunucu Güvenliği**

**Madde 12** - (1) Üniversite bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu kişiler tarafından yapılacaktır.

(2) Bütün sunucular ve mobil cihazlar Üniversite'nin cihaz envanterinde kayıtlı olmalıdır. Envanter en az sunucuların yeri ile sorumlu kişiyi ve donanım ve işletim sistemi bilgilerini içermelidir:

(3) Ana görevi ve üzerinde çalışan uygulamalar: İşletim sistemi versiyonları

(4) Üniversite bünyesinde izin verilen bilgi işlem sistemleri haricinde yabancı bir mobil cihaz ya da veri taşıyıcı takılamaz, kullanılamaz.

(5) Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

a) Genel Konfigürasyon Kuralları

1. İşletim sistemi konfigürasyonları BİDB'nin talimatlarına göre yapılacaktır.

2. Kullanılmayan servisler ve uygulamalar kapatılacaktır.

3. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti- virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi, arşivlenmesi ve yedeklenmesi sağlanmalıdır. Mümkünse, anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.

4. Uygulama erişimleri için standart güvenlik prensipleri çalıştırılmamalı ve gereksiz servisler açılmamalıdır.

5. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır.

6. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

7. Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar. Bu odalarda, yangın, sel baskını v.b. durumlara karşı önlemler alınmış olmalıdır.

8. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

b) Gözleme

1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:

2. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirler alınacaktır. Güvenlik ile ilgili olaylar, aşağıdakiler dahil ancak bunlarla sınırlı olmamak kaydıyla şu şekillerde olabilir:

- i. Port tarama atakları.
  - ii. Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
3. Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

c) Uygunluk

1. Denetimler, Komisyon tarafından yapılacak ve/veya yaptırılacak olup, bu denetimlerin sonucu [3] aylık periyodik aralıklarla Üniversite Yönetimine yazılı olarak bildirilecektir.

2. Denetimler BİDB tarafından yönetilecektir.

3. Denetimlerde organizasyonun işleyişine zarar verilmemesi için maksimum gayret gösterilecektir.

ç) İşletim

1. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

2. Sunucuların yazılım ve donanım bakımları yılda bir yetkili uzmanlar tarafından yapılmalıdır.

3. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

**Kimlik Doğrulama ve Yetkilendirme**

**Madde 13 - (1)** Bilgi sistemlerinde kimlik doğrulama ve yetkilendirme konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır:

a) Üniversite sistemlerine erişecek tüm kullanıcıların Kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.

b) Üniversite sistemlerine erişmesi gereken Üniversite dışı kullanıcılara yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.

c) Üniversite bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veri tabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkileri belirlenmelidir.

ç) Tüm Kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda yenilenmelidir.

d) Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.

e) Kullanıcılar, Üniversite adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.

f) Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

g) Sistemlere log-in olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

ğ) Kullanıcılara erişim hakları yazılı olarak bildirilmeli ve erişim haklarını ihlal eden kullanıcılar için yaptırım uygulanmalıdır.

h) Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır

**DÖRDÜNCÜ BÖLÜM**  
**Çeşitli ve Son Hükümler**

**Hüküm Bulunmayan Haller**

**Madde 14 - (1)** Bu Esaslarda hüküm bulunmayan hallerde; ilgili mevzuat hükümleri ile Yükseköğretim Kurulu, Senato ve ilgili Yönetim Kurulu Kararları uygulanır.

**Yürürlük**

**Madde 15 - (1)** Bu Esaslar, Senato tarafından kabul edildiği tarihten itibaren yürürlüğe girer.

**Yürütme**

**Madde 16 - (1)** Bu Esaslara ait hükümler, Toros Üniversitesi Rektörü tarafından yürütülür

<b>Esasların Kabul Edildiği Senato Kararının</b>	
<b>Tarihi</b>	<b>Sayısı</b>
29/05/2024	06/27
05/12/2024	10/52