HASAN KALYONCU ÜNİVERSİTESİ BİLGİ GÜVENLİĞİ YÖNERGESİ

1. **Amaç**

İşbu Bilgi Güvenliği Yönergesi ("**Yönerge**"), 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**KVKK**") uyarınca veri sorumlusu sıfatını haiz Hasan Kalyoncu Üniversitesi ("**Kurum**") nezdinde işlenen kişisel veri niteliğindeki verilerin korunması için bilgi güvenliği kapsamında uyulması gereken usul ve esasların belirlenmesi amacıyla düzenlenmiştir.
Yönerge, Senato/Rektörlük tarafından yürürlüğe sokulur ve gerektiğinde güncellenir.
Yönerge, Kurum'un Senato/Rektörlük tarafından yetkilendirilen Kişisel Veri Koruma Komisyonu ("**Komisyon**") tarafından uygulanır.

2. **Bilgi Güvenliği**

Bilgi güvenliği, Kurum'daki işlerin sürekliliğinin sağlanması, Kurum'un 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.

3. **Yönerge'nin Kapsamı**

İşbu Yönerge, Kurum bilgi işlem altyapısını kullanmakta olan tüm birimleri kapsar.

4. **Uygulama**

Kurum yönetimi, Kurum'un 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.

Söz konusu hedef doğrultusunda Komisyon, 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 Kurum, söz konusu olay hakkındaki delilleri toplayarak güvenli bir şekilde saklanmasını sağlar.

Kurum, yukarıdakiteknik ve idari tedbirler kapsamında çalışanlar ve öğrencilerin uyması için standartlar ve kurallar belirlemekte olup, bunlar aşağıdaki gibidir.

a) E-Posta Kullanma Kuralları

- Kurum'un 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.
- Kötü amaçlı, spam, sahte vs. nitelikteki zararlı elektronik postalara yanıt yazılmamalı, bu elektronik postalara iliştirilmiş her türlü çalıştırılabilir dosya içeren elektronik postalar alındığında hemen silinmeli ve kesinlikle başkalarına iletilmemelidir.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen elektronik postaların sahte elektronik posta olabileceği dikkate alınarak, herhangi bir işlem yapılmaksızın işbu elektronik postalar derhal silinmelidir.
- Çalışanlar ve öğrenciler, Kurum'un elektronik posta sistemi aracılığıyla uygun olmayan içerikleri (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb.) gönderemezler.
- 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.
- Kurum çalışanları ve öğrenciler, kurumsal elektronik postaların Kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görünmesi ve okunmasını engellemekten sorumludurlar.
- Kaynağı bilinmeyen elektronik posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmeli olup, bu şekilde gelen elektronik postalar Bilgi İşlem departmanına bildirilmelidir.

- Kullanıcılar kendilerine ait elektronik posta adresinin şifresinin güvenliğinden sorumludurlar. Şifrelerin kırıldığını fark ettikleri andan itibaren Kurum'un Bilgi İşlem departmanı ve Kişisel Verileri Koruma Komisyonu ile temasa geçip onlara durumu haber vermekle yükümlüdürler.
- Kurum'dan 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 Kurum ile ilişkisinin sona ermesi durumunda elektronik posta sisteminde gerekli değişiklikler yetkililer tarafından Bilgi İşlem departmanına 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

- Hiçbir kullanıcı, Kurum'un 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.)
- Kurum faaliyetleri kapsamında farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecek olması durumunda çalışanlar, bağlantılarının SSL ya da Bilgi İşlem departmanı tarafından belirlenecek olan daha güvenli bir yol ile gerçekleştirilmesinden sorumludur.
- Bilgisayarlar arası ağ üzerinden resmi görüşmeler haricinde mesajlaşma ve sohbet programları gibi mesajlaşma programları kullanılamaz.
- Hiçbir kullanıcı özel amaçlı olarak internet üzerinden Multimedia Streaming (Video, müzik ve iletişim vb. için) yapamaz.
- Kurum 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 Kurum'un veri depolama sistemlerine aktarılamaz, bu sistemlere kaydedilemez veya bu sistemlerde tutulamaz. Böyle bir işlemden, kişinin kendisi sorumlu olacak olup herhangi bir kişisel veri ihlalinde Kurum sorumlu tutulamayacaktır.
- İnternet üzerinden Kurum'un Bilgi İşlem departmanı tarafından onaylanmamış yazılımlar indirilemez ve Kurum sistemleri üzerine bu yazılımlar kurulamaz, kullanılamaz.
- Kurum ağlarından ve bilgisayarlarından genel ahlak anlayışına aykırı internet sitelerine girilmemeli ve dosya indirimi yapılmamalıdır.
- Bilgi İşlem departmanı, 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.
- Kurum'a ilişkin sistemler üzerinden herhangi bir siyasi içerik ya da propaganda paylaşımı yapılamaz.

c) Genel Kullanım Politikası

- 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.

- Kurum verilerini içeren bir bilgisayarın veya taşıyıcının çalınması, kaybolması gibi durumlarda, bu durum derhal ve herhalde en geç [24] saat içinde Bilgi İşlem departmanına ve Komisyon'a bildirilmelidir.
- Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek Kurum'a veya kişiye yönelik, elektronik bankacılık, hakaret veya siyasi içerikli mail, kullanıcı bilgileri ve bunun gibi saldırılardan kullanıcı sorumlu olacaktır.
- Kurum bilgisayarları aracılığıyla yasadışı olaylara karışılmamalıdır.
- 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.
- Kurum bilgileri ve bunun kapsayabileceği kişisel veriler, yetkili kişiler dışında ve ilgili kişinin açık onayı olmaksızın üçüncü kişilere aktarılmamalıdır.
- Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem departmanının onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.
- Herhangi bir cihaz, yazılım veya veri, Kurum'un faaliyetleri kapsamında gerekli olmadığı sürece izinsiz olarak Kurum dışına çıkarılmamalıdır. [Gerekli olduğu takdirde ise, [Bilgi İşlem departmanı] bu hususta bilgilendirilecektir.]
- Kurum'un kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları kullanmak yasaktır.
- Bilgi İşlem departmanı, 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. Kurum tarafından yasaklanmış veya herhangi bir sebeple silinerek kullanımdan kaldırılmış yazılım, donanım ve/veya servislerin çalışan ve öğrenciler tarafından Kurum bilgisayarları üzerinden kullanılması yasaktır.
- Çalışan ve öğrenciler, kendilerine tahsis edilen ve Kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki gerek kurumsal gerek kişisel verilerin güvenliğinden sorumludur. Bu doğrultuda, çalışanlar ve öğrenciler Kurum'un uygulamaya koyduğu politika, yönerge ve talimatlar doğrultusunda gerekli fiziki ve teknik önlemleri alır ve uygular.
- Bilgi İşlem departmanı kullanıcıya haber vermeksizin, Kurum'un faaliyetlerinin ve verilerinin güvenliğini sağlamak amacıyla, yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir, gereken teknik veya idari tedbirleri uygulayabilir.
- Kurum tarafından çalışanlara tahsis edilen cihazlarda ve bilgisayarlarda oyun ve eğlence amaçlı programlar kullanılamaz, çalıştırılamaz ve bu tarz program ve uygulamalar Kurum bilgisayarlarına kopyalanamaz.
- Bilgisayarlar üzerinden Kurum'un faaliyetleri kapsamında gerekli olanlar haricinde dosya alışverişinde bulunulmamalıdır.
- Kurum'da Bilgi İşlem departmanının bilgisi olmadan ağ sisteminde (Web Hosting, E-Posta Servisi vb.) sunucu niteliğinde olan bilgisayar ve cihaz bulundurulmamalıdır.
- Bilgi İşlem departmanının bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

- Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir. Lisanssız yazılımı Kurum tarafından kendisine tahsis edilen bilgisayarında barındıran çalışan veya Kurum bilgisayarını kullanan öğrenci veya çalışan, bu durumdan kendisi sorumludur.
- Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde mutlaka şifre kullanım kurallarına göre hareket edilmelidir.
- Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, problem hakkında ivedilikle Bilgi İşlem departmanına ve Kişisel Verileri Koruma Komisyonu'na haber verilmelidir.

d) Antivirüs Politikası

- Antivirüs yazılımı yüklü olmayan bilgisayar, ağa bağlanmamalı ve hemen Bilgi İşlem departmanına konu ile ilgili olarak haber verilmelidir.
- Zararlı programları (virüsler, solucanlar, truva atı, e-posta bombaları vb.) Kurum bünyesinde oluşturmak ve dağıtmak yasaktır.
- Hiçbir kullanıcı, herhangi bir sebepten dolayı Kurum tarafından kurulumu yapılmış olan antivirüs programını sistemden kaldıramaz ve bilgisayara başka bir antivirüs yazılımını kuramaz.
- Antivirüs yazılımlarını her daim güncel tutulacak olup, kullanıcıların söz konusu yazılımların güncelliğini etkileyecek işlemlerde bulunması yasaktır.

5. **Şifreleme**

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

- Uluslararası kabul gören şifreleme programları kullanılmalıdır.
- Kullanılan şifreler, kolayca kırılamayacak güce sahip olmalıdır.
- Şifreler (elektronik posta ve bilgisayar veya veri kayıt cihazına giriş için kullanılan her türlü şifre) en az [6] ayda bir değiştirilmelidir.
- Şifreler elektronik posta iletilerine veya herhangi bir elektronik forma yazılmamalı ve eklenmemeli, başkası ile paylaşılmamalı, fiziki ya da elektronik ortamlara yazılmamalıdır.
- Herhangi bir kişiye telefonda veya herhangi bir iletişim aracıyla şifre verilmemelidir.
- Şifreler, işten uzakta olunan zamanlarda dahi iş arkadaşlarıyla paylaşılmamalıdır.
- Şifre [3] defa üst üste yanlış girildiğinde bilgisayar kilitlenmelidir.
- Çoklu giriş yapılan bilgisayarlara giren personellere şifre kullanımı ve kişisel veri güvenliği hakkında uyarılar yapılmalıdır.

- Mutlaka ekran kilidi kullanılmalı ve ekranın [5] dakika hareketsiz kalması halinde ekran kilidi devreye girmelidir.
- Kurum bünyesinde kullanılan şifreler kurum dışında (bankacılık işlemleri vb.) herhangi bir şekilde kullanılmamalıdır.
- Değişik sistemler için farklı şifreleme kullanılmalıdır (örneğin, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanılmalıdır).
- Herhangi bir kimse şifre isteğinde bulunursa, kişi işbu Yönerge referans gösterilerek Bilgi İşlem departmanı ile Kişisel Verilerin Korunması Komisyonu'na yönlendirilmelidir.
- Uygulamalarda ve browser'lardaki "şifre hatırlama" özellikleri seçilmemelidir.

b) Şifre Oluşturma Kuralları

- Şifre; küçük ve büyük karakterler (a-z, A-Z) ile rakam ve semboller (0-9, !'^+%&/()=?_;* gibi) içermelidir.
- Şifre en az sekiz karakterden oluşmalıdır.
- Şifre oluşturulurken kolayca tahmin edilebilecek kombinasyonlardan kaçınılmalıdır.
- 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

- Herhangi bir kişiye telefonda şifre vermek.
- Elektronik posta mesajlarında şifre belirtmek.
- Üst yöneticiler ile şifre paylaşmak.
- Başkaları önünde şifreler hakkında konuşmak.
- Aile isimlerini şifre olarak kullanmak.
- Herhangi bir form üzerinde şifre belirtmek.
- Şifreleri aile bireyleri ile paylaşmak.
- Şifreleri işten uzakta olunan zamanlarda iş arkadaşlarına bildirmek.

d) Uygulama Geliştirme Standartları

- Uygulama geliştiricileri programları, veri bütünlüğünü bozma riskini minimize edecek nitelikte olup bireylerin (grupların değil) kimlik doğrulaması işlemini destekleyebilmelidir.
- Uygulama geliştiricileri programları, şifreleri 'text' olarak veya kolay anlaşılabilir formda saklamamalıdır.
- Uygulama geliştiricileri programlarının girdilerinin doğruluk ve uygunluk denetimini sağlamak amacıyla kontrol mekanizması yerleştirilmelidir.
- Uygulama geliştiricileri programları ile kural yönetim sistemi desteklenmelidir. Örneğin; bir kullanıcı diğer bir kimsenin şifresini bilmeden fonksiyonlarına devam edebilmelidir.

e) Uzaktan Erişim ve Aktarım

- Kurum’un bilgisayar ağına uzaktan erişimi tek yönlü şifreleme algoritması veya güçlü şifrelerle yapılmalıdır.
- Uzaktan erişim için iki kademeli kimlik doğrulama kontrolü uygulanmalıdır.
- Kurum’un 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.
- Bakım onarım gibi sebeplerle kişisel veri içeren cihazların üçüncü kişilere gönderilecek olması durumunda cihazlardaki veri saklama ortamları sökülerek güvenli bir yerde saklanmalıdır.
- Kurum faaliyetleri kapsamında üçüncü kişilere aktarılacak kişisel veriler, dikkatli bir şekilde ve Kurum’un belirleyeceği gerekli tedbirler alınarak gönderilmelidir.

6. **Yedekleme ve Bulutta Depolama**

- Kurum, çalışan ve öğrencilerin Kurum faaliyetleri kapsamında kullandığı elektronik cihazlardaki verileri kötü amaçlı yazılımlara karşı yedeklemekte olup, herhangi bir şekilde bir veri kaybı durumunda yedeklenen veriler faaliyete geçirilecektir.
- Yedeklenen verilere yalnızca sistem yöneticilerinin erişim yetkisi olup, yetkisiz kişilerce yedeklenmiş verilere erişilmesi yasaktır.
- 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.
- Bulutta depolanan kişisel verilerin içeriği detaylıca belirlenmeli, senkronizasyonu sağlanmalı ve bu veriler, kriptografik yöntemlerle şifrelenerek güvenli bir ortamda yedeklenmelidir.
- Bulut bilişim hizmet ilişkisi sona erdiğinde; bulutta depolanan kişisel verileri kullanılır hale getirmeye yarayabilecek şifreleme anahtarları ve bunların tüm kopyaları yok edilmelidir.

7. **Kişisel Veri İçeren Ortamların Güvenliği**

Kurumyerleşkesi içinde ve dışında yer alan ve Kurum bünyesinde kişisel veri içeren fiziksel ortamlar (kağıt 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, Kurum’un 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.

8. **Sunucu Güvenliği**

- Kurum bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu kişiler tarafından yapılacaktır.
- Bütün sunucular ve mobil cihazlar Kurum'un cihaz envanterinde kayıtlı olmalıdır. Envanter en az aşağıdaki bilgileri içermelidir:

1. Sunucuların yeri ve sorumlu kişi.
2. Donanım ve işletim sistemi.

- Ana görevi ve üzerinde çalışan uygulamalar.

1. İşletim sistemi versiyonları.

- Kurum bünyesinde izin verilen bilgi işlem sistemleri haricinde yabancı bir mobil cihaz ya da veri taşıyıcı takılamaz, kullanılamaz.
- Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

a) Genel Konfigürasyon Kuralları

- İşletim sistemi konfigürasyonları Bilgi İşlem departmanının talimatlarına göre yapılacaktır.
- Kullanılmayan servisler ve uygulamalar kapatılacaktır.
- Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- Uygulama erişimleri için standart güvenlik prensipleri çalıştırılmamalı ve gereksiz servisler açılmamalıdır.

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

- Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.
- Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.

b) Gözlemleme

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

- 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:

1. Port tarama atakları.
2. Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.

- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

c) Uygunluk

- Denetimler, Komisyon tarafından yapılacak ve/veya yaptırılacak olup, bu denetimlerin sonucu [3] aylık periyodik aralıklarla Kurum Yönetimine yazılı olarak bildirilecektir.
- Denetimler Bilgi İşlem Departmanı tarafından yönetilecektir.
- Denetimlerde organizasyonun işleyişine zarar verilmemesi için maksimum gayret gösterilecektir.

d) İşletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
- Sunucuların yazılım ve donanım bakımları yılda bir yetkili uzmanlar tarafından yapılmalıdır.
- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalıdır.

9. **Kimlik Doğrulama ve Yetkilendirme**

Bilgi sistemlerinde kimlik doğrulama ve yetkilendirme konusunda alınması gereken

önlemler, uyulması gereken kurallar ve standartlar şunlardır:

- Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecektir.
- Kurum sistemlerine erişmesi gereken kurum dışı kullanıcılara yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacaktır.
- Kurum 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.
- 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 revize edilmelidir.
- Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.
- Kullanıcılar, Kurum adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.

- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere log-in olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.
- Kullanıcılara erişim hakları yazılı olarak bildirilmeli ve erişim haklarını ihlal eden kullanıcılar için yaptırım uygulanmalıdır.
- Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

10. **Yönerge'nin Uygulanması**

İşbu Yönerge, Komisyon tarafından uygulanır.