

# Güvenlik Yönetimi, Uygulama Geliştirme Güvenliği, İş Sürekliliği Planlaması

Dr. Gülbahar  
AKGÜN



# **Güvenlik Yönetimine Giriş ve Temel Kavramlar**



**Güvenlik yönetimi,** bir organizasyonun bilgi varlıklarını korumak amacıyla tasarlanmış politikalar, süreçler ve uygulamalardan oluşur. Amacı, bilgi güvenliği risklerini tanımlamak, yönetmek ve azaltmaktır.

**Bilgi Koruma:** Verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaya yönelik stratejilerin oluşturulması.

**Hukuki Yükümlülükler:** Yasal düzenlemelere (örneğin, KVKK, GDPR) uyum sağlamak.

**İtibar Yönetimi:** Güvenlik açıklarının neden olduğu olumsuz durumların, kurumsal itibar üzerinde yarattığı olumsuz etkilerin azaltılması.

**Süreklilik:** İş sürekliliği için gerekli olan güvenlik önlemlerinin alınması.



Bilgi güvenliği, üç temel ilke üzerine kuruludur:

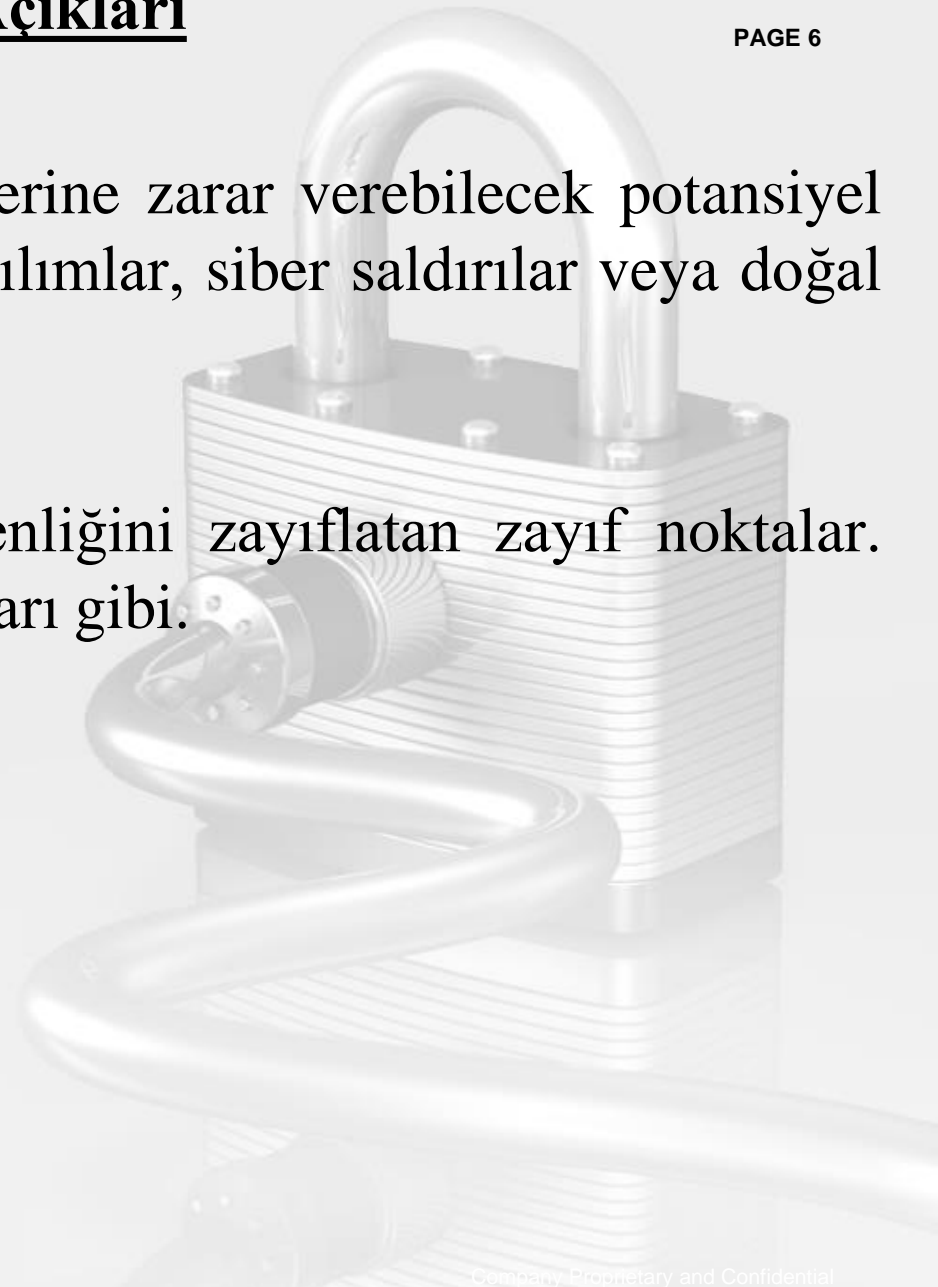
**Gizlilik:** Bilgilerin yalnızca yetkili kişiler tarafından erişilmesini sağlar. Şifreleme ve erişim kontrolü gibi yöntemler kullanılır.

**Bütünlük:** Verilerin doğruluğunu ve tutarlılığını korumaya yönelik önlemlerdir. Verilerin yetkisiz değişikliklerden korunması sağlanır.

**Erişilebilirlik:** Yetkili kullanıcıların bilgilere zamanında ve güvenli bir şekilde ulaşabilmesini garanti eder.

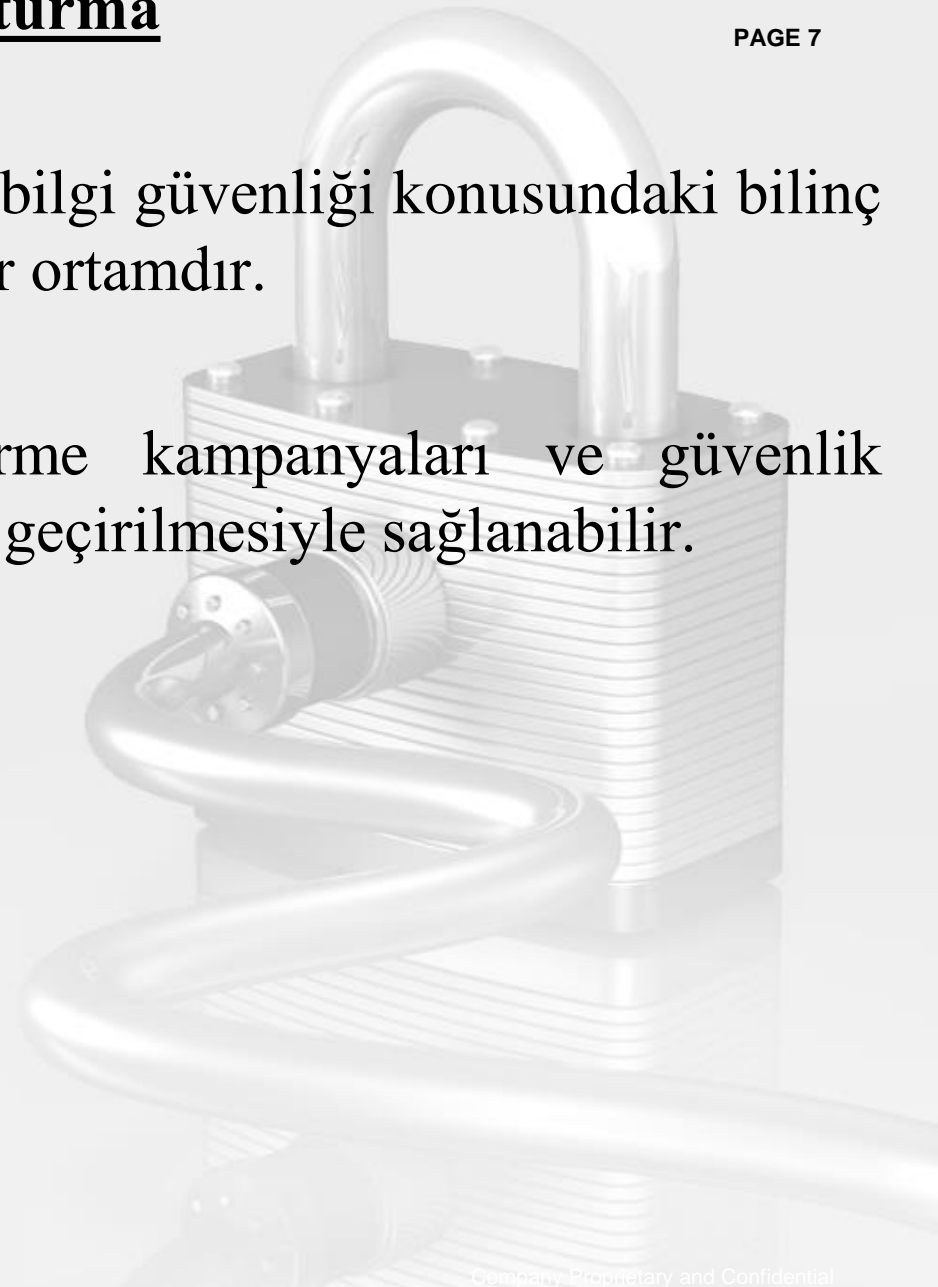
**Güvenlik Tehditleri:** Bilgi sistemlerine zarar verebilecek potansiyel olaylardır. Örneğin, kötü niyetli yazılımlar, siber saldırılar veya doğal afetler.

**Güvenlik Açıkları:** Sistemin güvenliğini zayıflatan zayıf noktalar. Yazılım hataları, zayıf şifre politikaları gibi.



**Güvenlik kùltürü**, tüm çalıřanların bilgi güvenlięi konusundaki bilinç düzeyini artırmak için oluřturulan bir ortamdır.

Bu, düzenli eęitimler, bilgilendirme kampanyaları ve güvenlik politikalarının sürekli olarak gözden geçirilmesiyle sağlanabilir.



# **Risk Yönetimi ve Kullanımları**





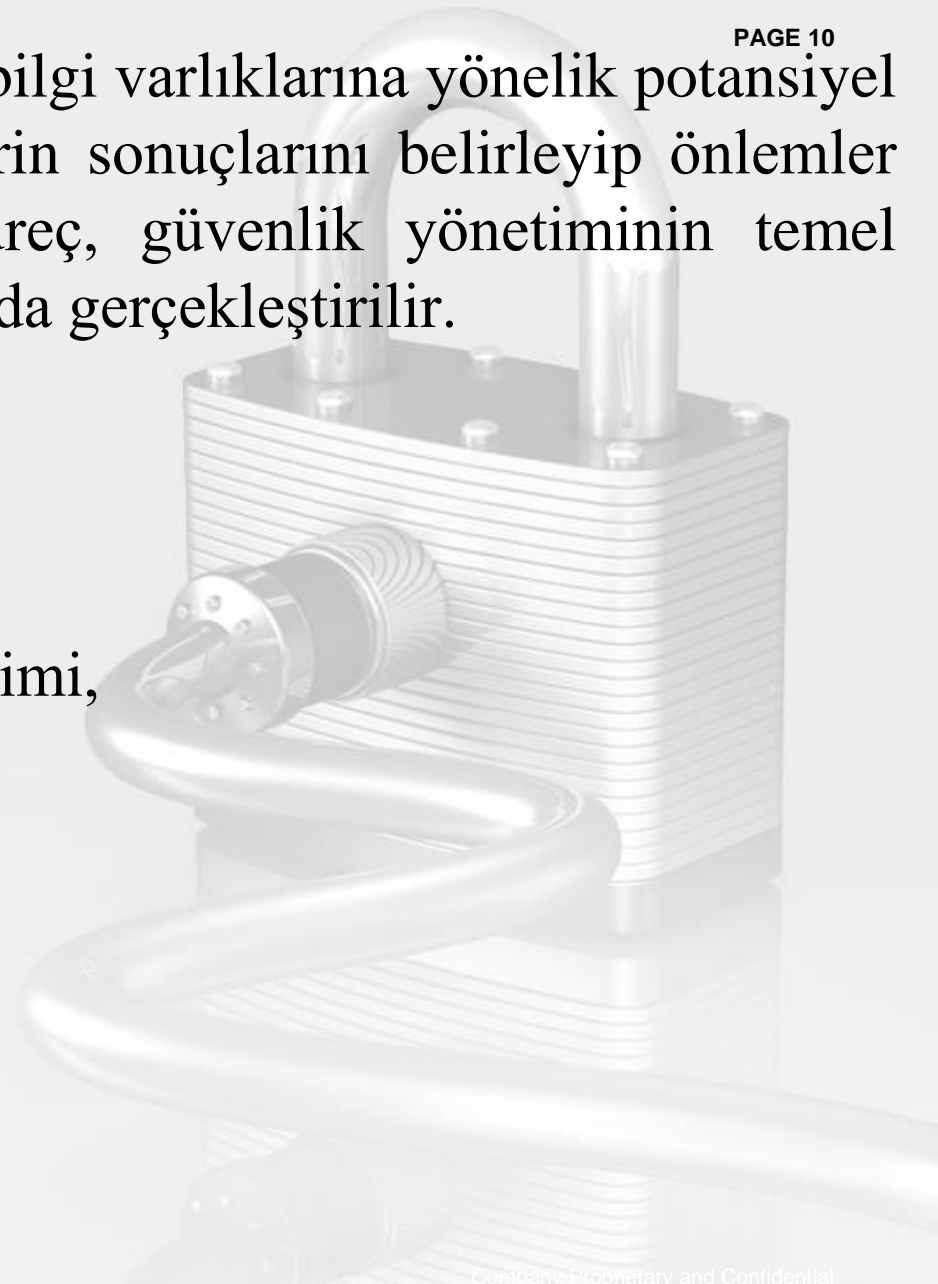
**Risk Analizi:** Kurumun karşılaşılabileceği tehditleri, zafiyetleri ve potansiyel riskleri belirlemek için sistematik bir analiz süreci açıklanmalıdır.

**Risk Değerlendirme ve Önceliklendirme:** Risklerin etkileri değerlendirilerek hangi risklerin öncelikle ele alınması gerektiği belirlenmelidir.

**Risk Azaltma Stratejileri:** Riskleri azaltmak veya ortadan kaldırmak için hangi güvenlik önlemlerinin alınacağı, yani riskten kaçınma, riskin etkisini azaltma, riski kabul etme ya da riski devretme gibi stratejiler açıklanmalıdır.

**Risk yönetimi**, bir organizasyonun bilgi varlıklarına yönelik potansiyel tehditleri, zafiyetleri ve bu tehditlerin sonuçlarını belirleyip önlemler almasını sağlayan süreçtir. Bu süreç, güvenlik yönetiminin temel taşlarından biridir ve dört ana aşamada gerçekleştirilir.

- Risk Tanımlama,
- Risk Değerlendirme,
- Risk Azaltma ve Kontrollerin Seçimi,
- İzleme ve Değerlendirme



## a) Risk Tanımlama

**Tehditlerin ve Zafiyetlerin Belirlenmesi:** Organizasyonun varlıkları üzerindeki potansiyel tehditler (örneğin, siber saldırılar, veri kaybı, doğal afetler) ve zafiyetler (sistem açıkları, yetersiz güvenlik önlemleri) tespit edilir.

**Varlıkların Değerinin Belirlenmesi:** Hangi bilgi varlıklarının korunması gerektiği ve bu varlıkların ne kadar kritik olduğu değerlendirilir. Bu sayede, hangi risklerin daha öncelikli ele alınması gerektiği anlaşılır.

## b) Risk Değerlendirme

**Risk Etkisi ve Olasılık Analizi:** Belirlenen risklerin kuruma olan etkisi ve gerçekleşme olasılığı değerlendirilir. Bu analizler, sayısal veya niteliksel yöntemlerle yapılabilir (örneğin, düşük-orta-yüksek gibi kategorilerle veya finansal etki olarak).

**Risk Önceliklendirme:** Etki ve olasılık analizine göre riskler önceliklendirilir. En yüksek etki ve olasılığa sahip riskler, acil olarak ele alınır.

## c) Risk Azaltma ve Kontrollerin Seçimi

PAGE 13

**Kontrol Stratejilerinin Belirlenmesi:** Risklerin etkisini azaltmak için kullanılacak güvenlik kontrolleri belirlenir. Bu kontroller, riskin etkisini azaltma, riski devretme (sigorta yoluyla), riskten kaçınma veya riski kabul etme gibi stratejiler içerir.

**Önleyici ve Caydırıcı Kontrollerin Uygulanması:** Tehditlerin önüne geçmek ve olası zararları azaltmak için güvenlik duvarları, kimlik doğrulama mekanizmaları, veri şifreleme gibi teknik kontroller uygulanır.

## d) İzleme ve Değerlendirme

PAGE 14

**Düzenli Risk Değerlendirmesi ve Güncellemeler:** Organizasyon, risk ortamındaki değişiklikleri düzenli olarak izleyerek risk yönetim süreçlerini günceller.

**Performans Göstergeleri ve Denetim:** Risk yönetiminin etkinliği, belirli performans göstergeleri aracılığıyla değerlendirilir. Ayrıca, iç ve dış denetimlerle risk yönetiminin güncel ve etkin kalması sağlanır.

# **Güvenlik Politikaları ve Prosedürleri**



**Güvenlik Politikaları ve Prosedürleri**, bir kuruluşun bilgi güvenliği hedeflerini, standartlarını ve uygulama süreçlerini belirleyen kapsamlı bir kılavuz sunar.

Güvenlik politikaları, kurumların bilgi varlıklarını koruma, güvenlik açıklarını minimize etme ve siber tehditlere karşı hazırlıklı olma amacını güder.

Bu politikaların uygulanması, tüm çalışanlar ve sistemler için bağlayıcı kurallar sunarak organizasyonel güvenliği artırır.



# Güvenlik Politikaları Nedir?

**Güvenlik Politikası**, bir kurumun bilgi güvenliği hedeflerini, kurallarını ve bu hedeflere ulaşmak için izleyeceği yöntemleri tanımlar.

Bu politikaların temel amacı, organizasyonun bilgi varlıklarını; gizlilik, bütünlük ve erişilebilirlik prensipleri çerçevesinde koruma altına almaktır.

Güvenlik politikaları, organizasyonun genel güvenlik çerçevesini oluşturur ve tüm çalışanlara, güvenlik risklerinin nasıl ele alınacağını öğretir.

- 1. Bilgi Varlıklarını Korumak:** Yetkisiz erişim, veri ihlalleri veya veri kaybına karşı kuruluşun bilgi varlıklarını koruma altına almak.
- 2. Yasal Uyumluluğu Sağlamak:** KVKK, GDPR ve ISO 27001 gibi yasal düzenlemelere uyumlu olarak çalışmak.
- 3. Siber Tehditlere Karşı Savunma Geliştirmek:** Potansiyel siber saldırılara karşı önleyici tedbirler almak.
- 4. İş Sürekliliğini Sağlamak:** Kriz veya saldırı anında organizasyonel faaliyetlerin sürdürülebilirliğini sağlamak.

Güvenlik politikaları, organizasyonun ihtiyaçlarına ve odaklandığı alanlara göre çeşitlenebilir. Başlıca güvenlik politikası türleri şunlardır:

- 1. Bilgi Güvenliği Politikası:** Bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini koruma amacını güder. Bu politika, organizasyonun bilgi güvenliği standartlarını tanımlar.
- 2. Erişim Kontrol Politikası:** Çalışanların erişim yetkilerini belirler ve hangi bilgiye, kimlerin hangi seviyede erişebileceğini düzenler. Özellikle yetkisiz erişimlerin engellenmesi açısından kritiktir.

**3. Yedekleme ve Felaket Kurtarma Politikası:** Verilerin düzenli olarak yedeklenmesi ve olası bir veri kaybı durumunda hızlıca geri yüklenmesi için gereken adımları açıklar.

**4. Kabul Edilebilir Kullanım Politikası (AUP):** Çalışanların hangi yazılımları, cihazları ve internet kaynaklarını hangi şartlarda kullanabileceğini düzenler. AUP, kişisel cihazların (BYOD) kullanımını gibi konuları da kapsar.

**5. Şifre Yönetimi Politikası:** Güçlü şifrelerin oluşturulması, periyodik olarak değiştirilmesi ve yönetilmesi için kurallar koyar. Örneğin, şifrelerin karmaşık olması, sıkça güncellenmesi gibi.

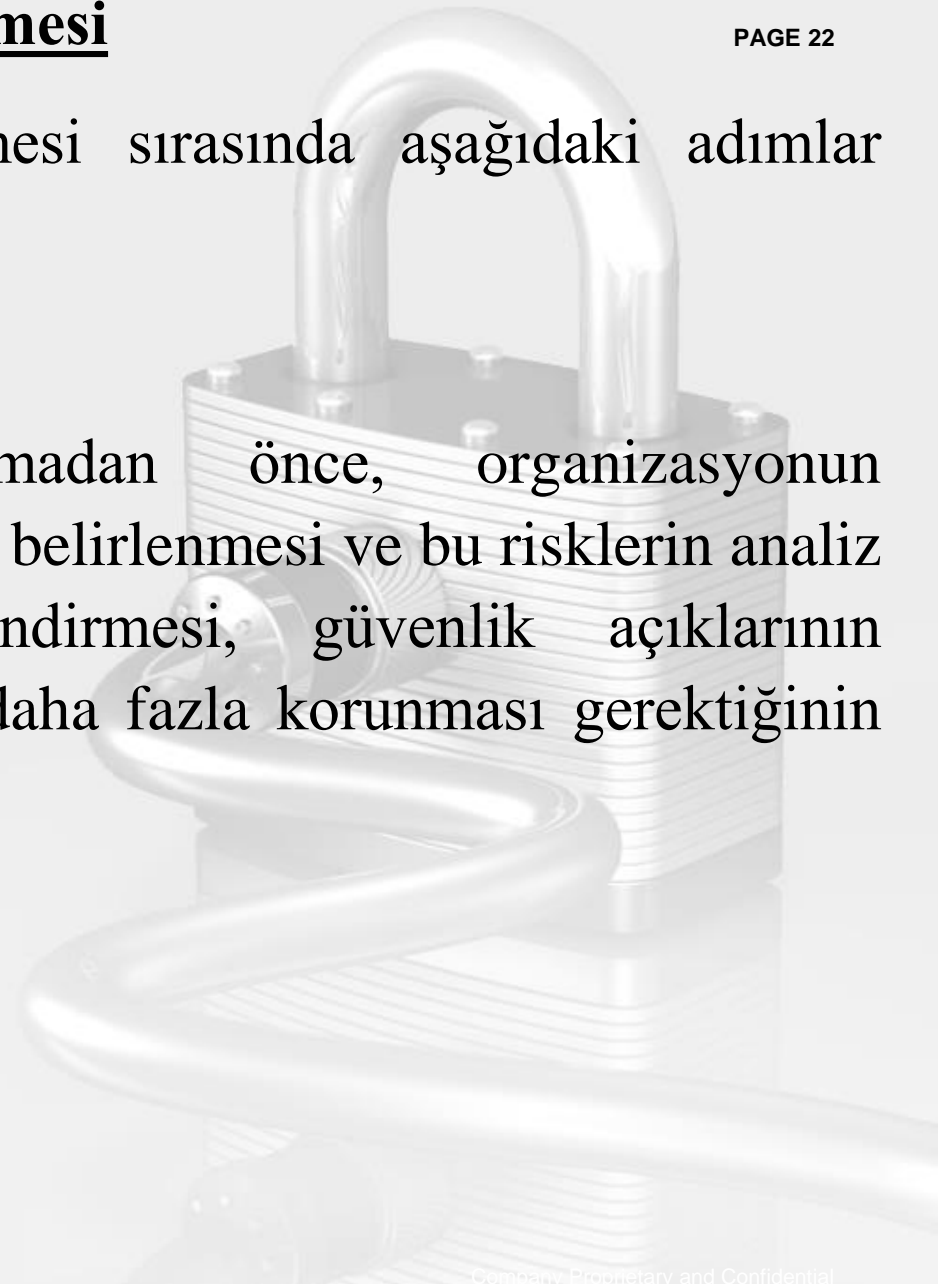
**6. Mobil Cihaz Güvenliği Politikası:** Çalışanların mobil cihazları güvenli bir şekilde kullanmalarını sağlar. Bu politika özellikle uzaktan çalışma ve mobil çalışma ortamları için önemlidir.

**7. Ağ Güvenliği Politikası:** Ağ güvenliği için alınması gereken önlemleri ve kullanılan güvenlik teknolojilerini açıklar. Bu politika, güvenlik duvarları, VPN'ler ve ağ segmentasyonu gibi konuları içerir.

Güvenlik politikalarının geliştirilmesi sırasında aşağıdaki adımlar izlenir:

## **A. Risk Değerlendirmesi**

Güvenlik politikaları oluşturulmadan önce, organizasyonun karşılaşılabileceği potansiyel risklerin belirlenmesi ve bu risklerin analiz edilmesi gerekir. Risk değerlendirmesi, güvenlik açıklarının tanımlanması ve hangi varlıkların daha fazla korunması gerektiğinin belirlenmesine yardımcı olur.



## **B. Standartların ve Düzenlemelerin İncelenmesi**

PAGE 23

Güvenlik politikaları oluşturulurken ISO 27001, COBIT, NIST gibi güvenlik standartlarına ve KVKK, GDPR gibi yasal düzenlemelere uyulması önemlidir. Bu standartlar ve düzenlemeler, organizasyonların güvenlik politikalarını daha sistematik ve yasal olarak sağlam hale getirir.

## **C. Politika Belirleme ve Dokümantasyon**

Güvenlik politikalarının oluşturulması sürecinde tüm kurallar, yetkiler ve sorumluluklar açıkça tanımlanır. Bu kurallar ve uygulamalar, bir doküman olarak hazırlanır ve tüm çalışanlara erişim sağlanır.

## **D. Politika Eğitimi ve Bilgilendirme**

PAGE 24

Güvenlik politikalarının tüm çalışanlar tarafından anlaşılması ve uygulanması önemlidir. Bu nedenle, çalışanlara güvenlik politikaları hakkında düzenli olarak eğitimler verilir ve güvenlik farkındalığı artırılır.

## **E. Politikaların Periyodik İncelenmesi**

Siber güvenlik tehditleri sürekli değiştiğinden, güvenlik politikalarının da düzenli olarak güncellenmesi gerekir. Belirli aralıklarla yapılan gözden geçirmelerle, politikaların güncelliği sağlanır.



# Güvenlik Prosedürleri Nedir?

**Güvenlik Prosedürleri**, güvenlik politikalarının uygulanmasını sağlayan adım adım talimatlardır. Prosedürler, güvenlik politikalarını hayata geçirmek için izlenen yöntemler ve teknik detayları içerir. Örneğin, bir şifre yönetim politikasına uygun olarak, şifrelerin nasıl oluşturulacağı, saklanacağı ve korunacağına dair adımlar bir prosedür şeklinde tanımlanır.

## Örnek Güvenlik Prosedürleri

- 1. Erişim Talebi Prosedürü:** Çalışanların, belirli bir bilgiye erişim yetkisi talep etme adımlarını ve bu taleplerin nasıl onaylanacağını tanımlar.

**2. Olay Müdahale Prosedürü:** Güvenlik ihlali veya siber saldırı durumunda izlenecek adımları belirler. Bu prosedür, bir saldırı durumunda sorumlu kişilerin görevlerini ve olayın nasıl yönetileceğini içerir.

**3. Veri Yedekleme ve Geri Yükleme Prosedürü:** Verilerin düzenli olarak nasıl yedekleneceğini, yedeklerin nasıl saklanacağını ve veri kaybı durumunda nasıl geri yükleneceğini açıklar.

# **Güvenlik Politikalarının ve Prosedürlerinin Uygulanmasının Faydaları**

- 1. Güvenlik Açıklarının Azaltılması:** Politikalar ve prosedürler, güvenlik risklerini azaltmak ve bilgi varlıklarını korumak için önleyici adımlar sunar.
- 2. Yasal Uyumluluk Sağlanması:** KVKK, GDPR gibi düzenlemelere uyum sağlanması, olası cezaların önüne geçilmesini sağlar.
- 3. Çalışan Farkındalığını Artırma:** Çalışanlar, güvenlik politikalarına ve prosedürlere bağlı kalarak siber tehditlere karşı daha hazırlıklı hale gelir.

**4. Veri İhlallerini Engelleme:** Politikalar ve prosedürler, veri ihlali gibi durumları önlemek için yapılandırılmış bir güvenlik çerçevesi sunar.

**5. Siber Saldırlara Karşı Dayanıklılığı Artırma:** İyi bir güvenlik politikasına sahip olan kurumlar, siber saldırılara karşı daha dirençli olur ve olası zararları minimize edebilir.



Siber güvenlik tehditleri ve organizasyonel yapılar sürekli değiştiği için, güvenlik politikalarının ve prosedürlerinin periyodik olarak güncellenmesi önemlidir. Aşağıdaki durumlarda güvenlik politikaları gözden geçirilmelidir:

- **Yeni Tehditlerin Ortaya Çıkması:** Yeni bir siber tehdit veya güvenlik açığı ortaya çıktığında politikalar güncellenmelidir.
- **Organizasyonel Değişiklikler:** Yeni bir teknoloji, sistem veya süreç organizasyona entegre edildiğinde ilgili güvenlik politikaları yeniden ele alınmalıdır.
- **Yasal Düzenlemelerdeki Değişiklikler:** KVKK veya GDPR gibi yasal düzenlemelerde değişiklikler olduğunda güvenlik politikaları bu yeni düzenlemelere uygun hale getirilmelidir.

# Güvenlik Politikaları ve Prosedürleri İçin Örnek Araçlar ve Yöntemler

Güvenlik politikalarının oluşturulması ve yönetimi için çeşitli araç ve yöntemler kullanılabilir:

- 1. Politika Yönetim Yazılımları:** Birçok organizasyon, güvenlik politikalarını yönetmek için özel yazılımlar kullanır. Bu yazılımlar, politika oluşturma, güncelleme ve çalışanlara duyurma süreçlerini kolaylaştırır.
- 2. Olay Yönetim Sistemleri:** Güvenlik olaylarının kaydedilmesi ve analiz edilmesi için olay yönetim yazılımları kullanılır.
- 3. Denetimler ve Güvenlik Raporlamaları:** Güvenlik politikalarının ve prosedürlerinin etkinliğini ölçmek için düzenli olarak iç ve dış denetimler yapılır. Bu denetimler sayesinde politikalar gözden geçirilir ve iyileştirmeler yapılır.

# **Farkındalık Eğitimleri ve Güvenlik Kültürü**



**Farkındalık Eğitimleri ve Güvenlik Kültürü**, bir organizasyondaki tüm bireylerin bilgi güvenliği risklerinin farkında olmalarını sağlamak ve güvenlik sorumluluğunu paylaşmalarını teşvik etmek amacıyla düzenlenmiş kapsamlı programlardır.

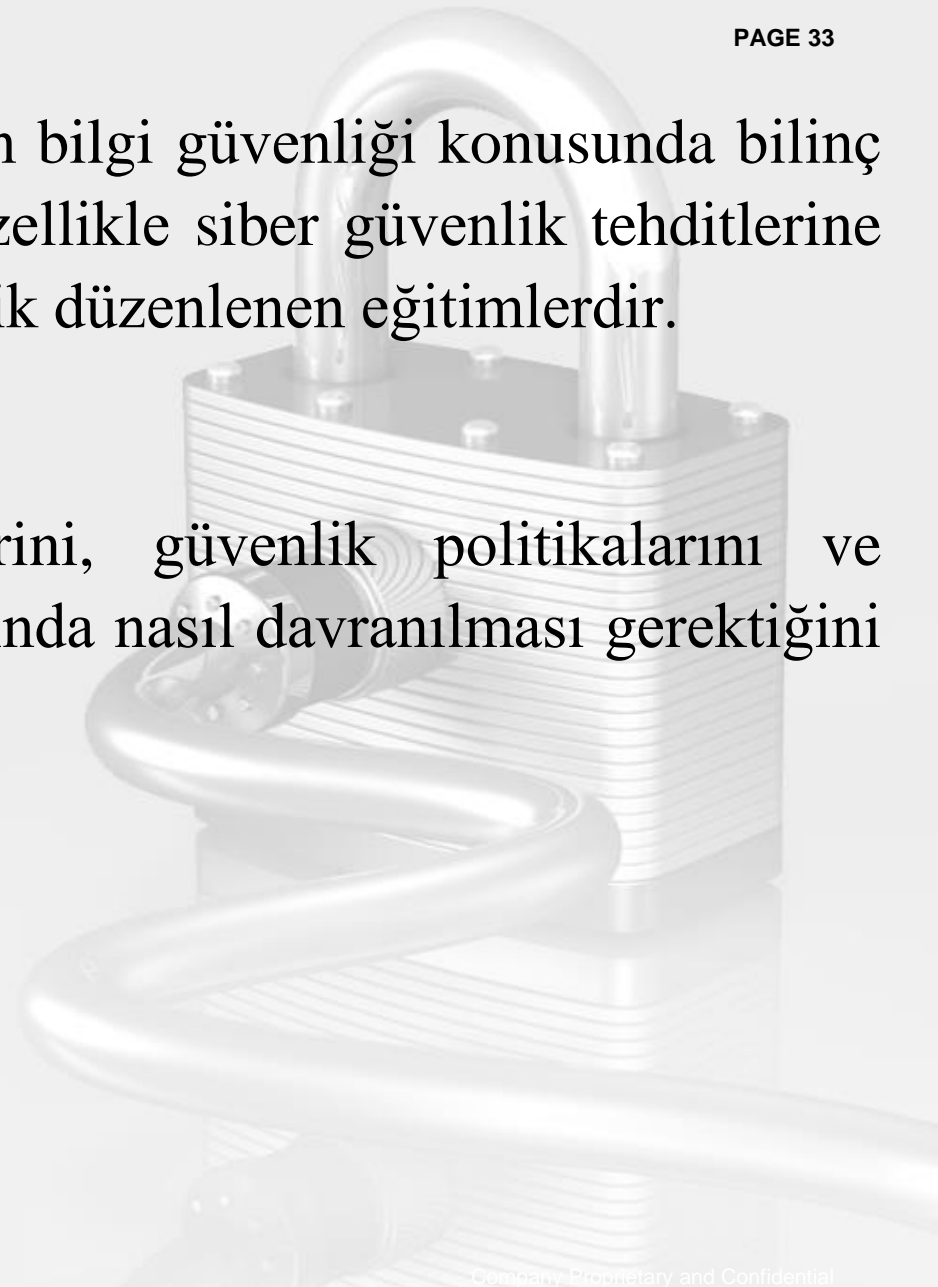
Bu tür eğitimler, çalışanların güvenlik tehditlerini tanımasını, uygun güvenlik davranışlarını benimsemesini ve güvenlik politikalarına uymasını sağlayarak organizasyonel güvenlik seviyesini artırır.



# Farkındalık Eğitimleri Nedir?

**Farkındalık Eğitimleri**, çalışanların bilgi güvenliği konusunda bilinç düzeylerini artırmayı hedefleyen, özellikle siber güvenlik tehditlerine karşı farkındalığı geliştirmeye yönelik düzenlenen eğitimlerdir.

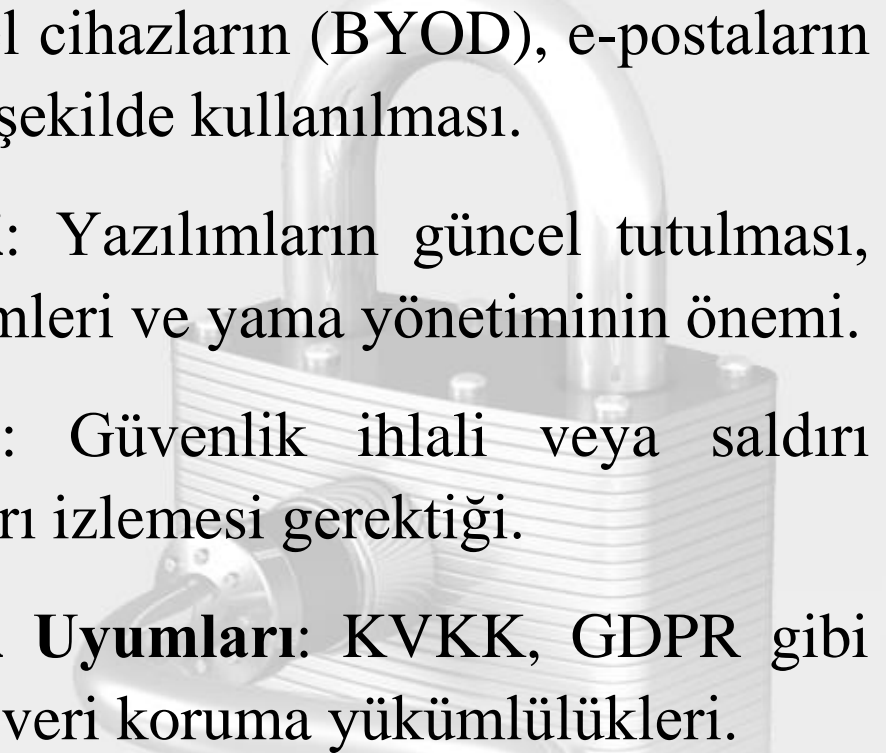
Eğitimler, bilgi güvenliği ilkelerini, güvenlik politikalarını ve potansiyel güvenlik tehditleri karşısında nasıl davranılması gerektiğini kapsamaktadır.



- 1. Güvenlik Bilincini Artırmak:** Çalışanları güvenlik tehditleri konusunda bilinçlendirmek, siber saldırılara karşı savunmasız davranışları azaltmak.
- 2. Riskleri Minimize Etmek:** İnsan hatalarını en aza indirerek, kurum içindeki güvenlik risklerini azaltmak.
- 3. Kurumsal Güvenlik Politikalarına Uyum Sağlamak:** Çalışanların güvenlik politikalarına ve yasal düzenlemelere uymasını sağlamak.
- 4. Güvenlik Kültürünü Yaygınlaştırmak:** Organizasyon genelinde bir güvenlik kültürü oluşturmak.

Farkındalık eğitimlerinde işlenen başlıca konular şunlardır:

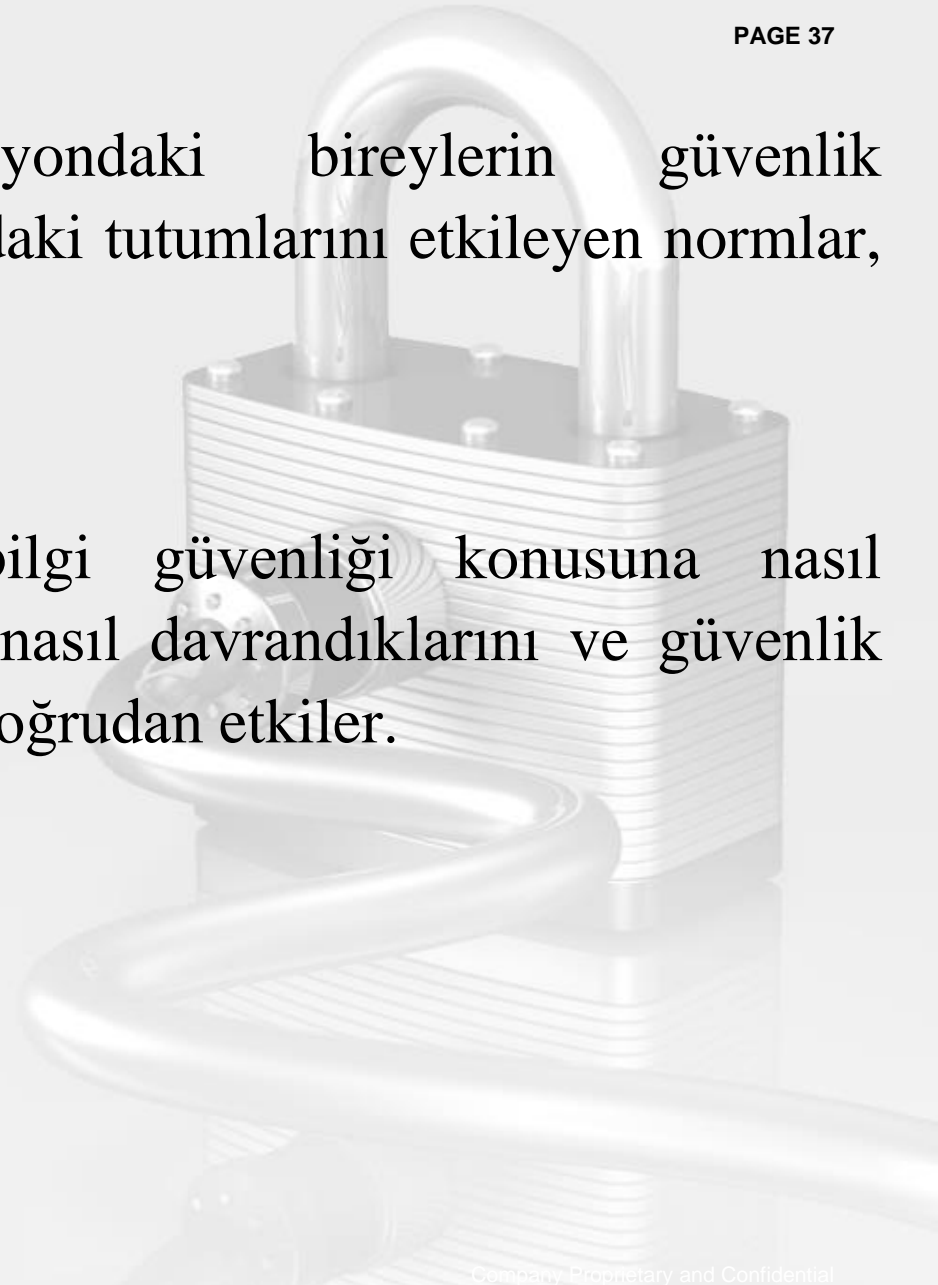
- 1. Temel Bilgi Güvenliği Prensipleri:** Gizlilik, bütünlük ve erişilebilirlik gibi temel güvenlik prensiplerinin önemi.
- 2. Parola Güvenliği:** Güçlü ve karmaşık parolaların nasıl oluşturulacağı ve saklanacağı.
- 3. Kimlik Avı (Phishing) ve Sosyal Mühendislik:** Çalışanların kimlik avı saldırılarını tanıması ve sosyal mühendislik saldırılarına karşı dikkatli olması.

- 
- 4. Güvenli Cihaz Kullanımı:** Kişisel cihazların (BYOD), e-postaların ve çevrimiçi kaynakların güvenli bir şekilde kullanılması.
- 5. Yazılım ve Güncelleme Bilinci:** Yazılımların güncel tutulması, zararlı yazılımlardan korunma yöntemleri ve yama yönetiminin önemi.
- 6. Olay Müdahale Prosedürleri:** Güvenlik ihlali veya saldırı durumunda çalışanların hangi adımları izlemesi gerektiği.
- 7. Veri Koruma ve Gizlilik Yasal Uyumları:** KVKK, GDPR gibi yasal düzenlemelere uyum ve kişisel veri koruma yükümlülükleri.

# Güvenlik Kültürü Nedir?

**Güvenlik Kültürü**, organizasyondaki bireylerin güvenlik davranışlarını ve güvenlik konusundaki tutumlarını etkileyen normlar, inançlar ve değerler bütünüdür.

Güvenlik kültürü, çalışanların bilgi güvenliği konusuna nasıl yaklaştıklarını, tehditler karşısında nasıl davrandıklarını ve güvenlik politikalarına ne kadar uyduklarını doğrudan etkiler.



- 1. Paylaşılmış Güvenlik Sorumluluğu:** Güvenlik kültürü olan bir organizasyonda tüm çalışanlar güvenliğin yalnızca BT biriminin sorumluluğu olmadığını, herkesin katkıda bulunması gereken bir alan olduğunu bilir.
- 2. Güvenlik Bilinci ve Duyarlılık:** Çalışanlar, güvenlik açıklarını ve siber tehditleri tanımakta, bu tehditler karşısında uygun güvenlik önlemlerini almakta daha hassastır.
- 3. Davranışsal Güvenlik Yöntemleri:** Çalışanlar, güvenlik eğitimlerinde öğrendikleri davranışları günlük iş süreçlerinde uygulayarak güvenlik tehditlerini minimize eder.

**4. Öğrenme ve Uyarlanabilirlik:** Güvenlik kültürü olan organizasyonlar, siber tehditlerdeki değişikliklere uyum sağlamak için sürekli öğrenme ve gelişim sağlar.

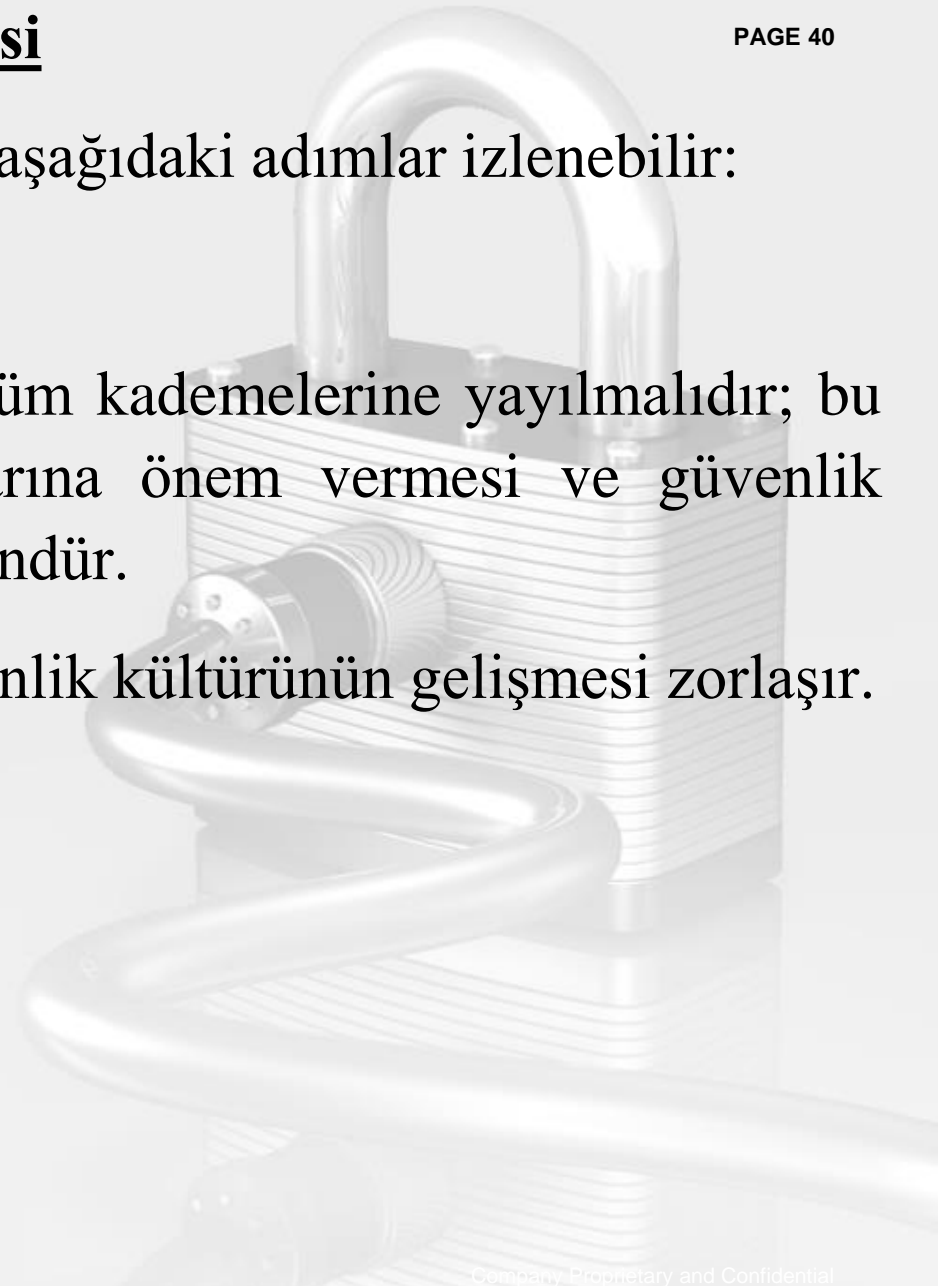
**5. Açıklık ve Güvenlik İhlallerini Bildirme:** Çalışanlar güvenlik ihlallerini veya olası güvenlik açıklarını bildirme konusunda cesaretlendirilir ve bu tür bildirimlerde bulunmaları teşvik edilir.

Güvenlik kültürünü geliştirmek için aşağıdaki adımlar izlenebilir:

## **A. Üst Yönetim Desteği**

Güvenlik kültürü, organizasyonun tüm kademelerine yayılmalıdır; bu da üst yönetimin güvenlik konularına önem vermesi ve güvenlik önlemlerini teşvik etmesi ile mümkündür.

Üst yönetimin desteği olmadan güvenlik kültürünün gelişmesi zorlaşır.



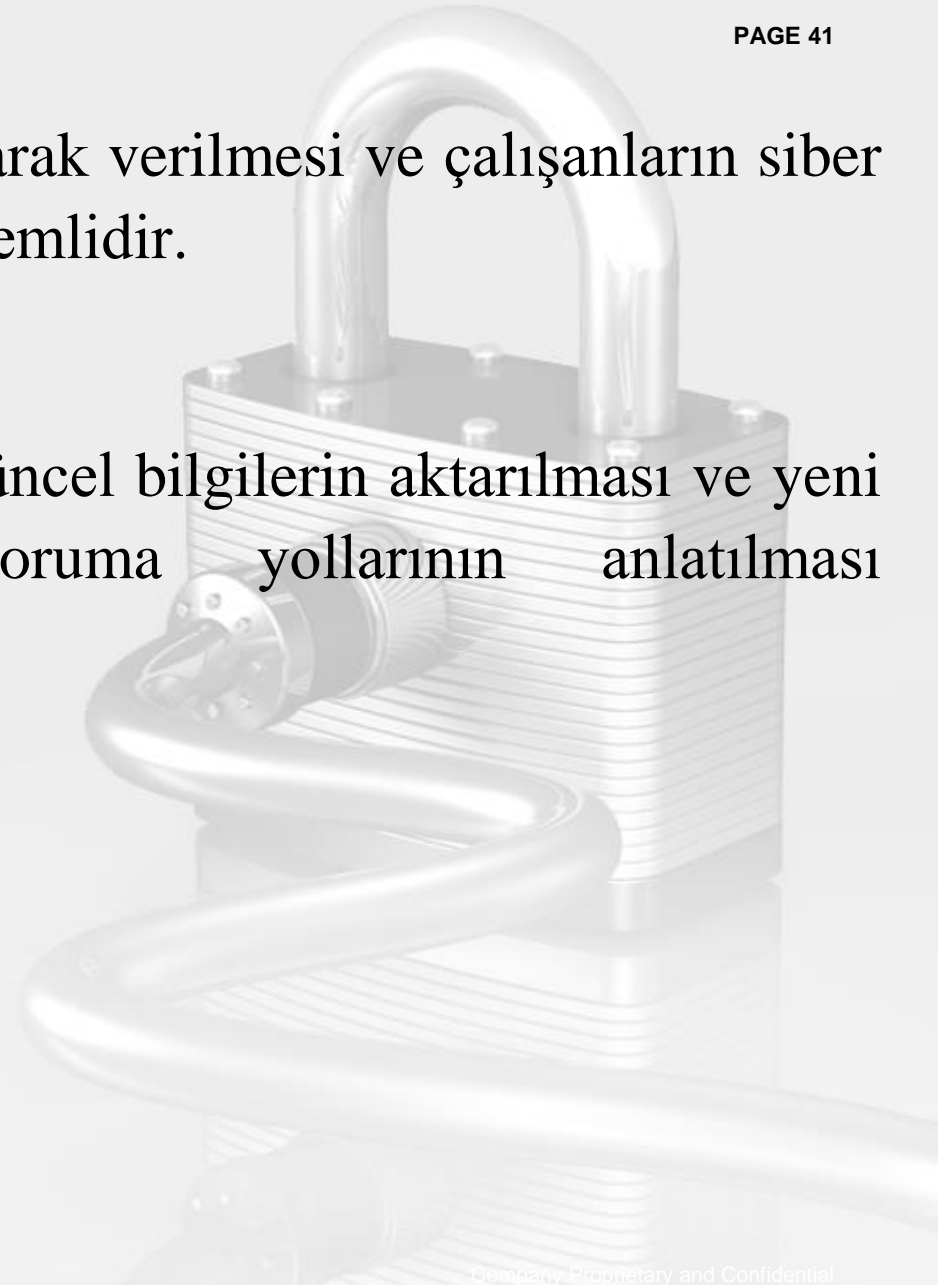


## B. Düzenli Farkındalık Eğitimi

PAGE 41

Farkındalık eğitimlerinin düzenli olarak verilmesi ve çalışanların siber tehditlere karşı bilinçlendirilmesi önemlidir.

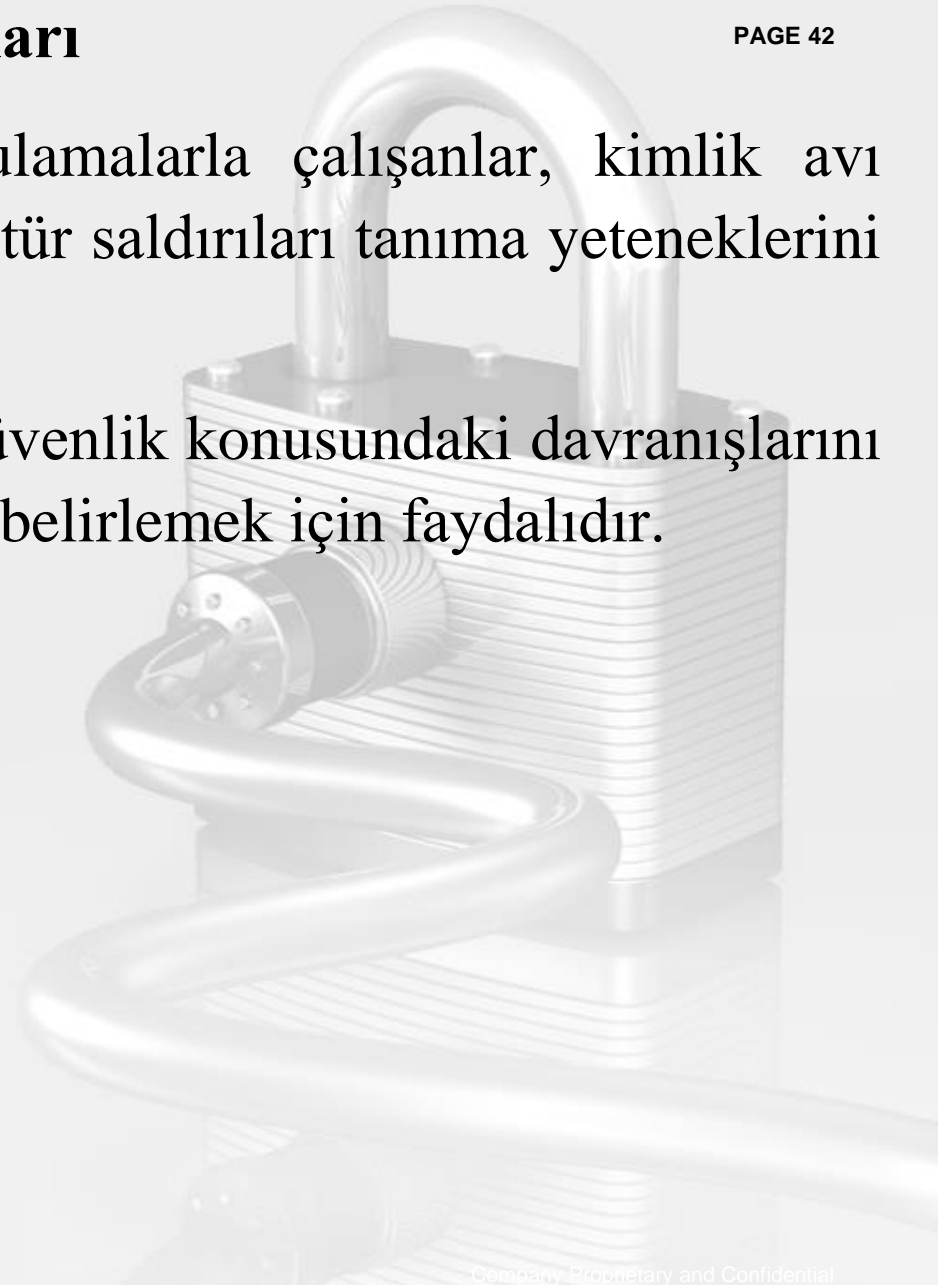
Eğitimlerde, siber tehditlere karşı güncel bilgilerin aktarılması ve yeni saldırı yöntemlerine karşı koruma yollarının anlatılması gerekmektedir.



## C. Gerçekçi Güvenlik Simülasyonları

Phishing simülasyonları gibi uygulamalarla çalışanlar, kimlik avı saldırılarına karşı pratik yaparak bu tür saldırıları tanıma yeteneklerini geliştirirler.

Bu tür simülasyonlar, çalışanların güvenlik konusundaki davranışlarını gözlemlemek ve eğitim ihtiyaçlarını belirlemek için faydalıdır.

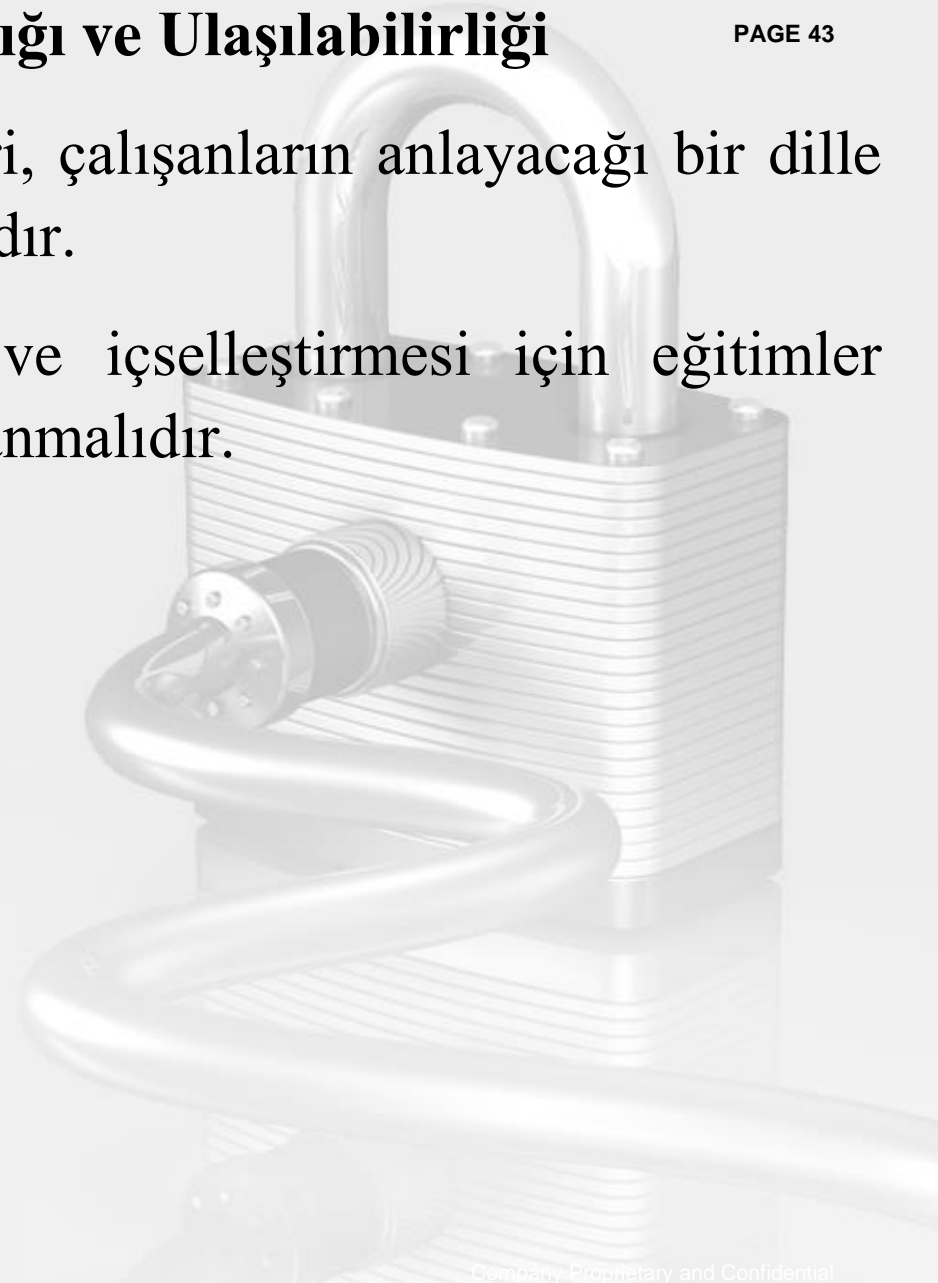


## **D. Güvenlik Politikalarının Şeffaflığı ve Ulaşılabilirliği**

PAGE 43

Güvenlik politikaları ve prosedürleri, çalışanların anlayacağı bir dille yazılmalı ve kolay erişilebilir olmalıdır.

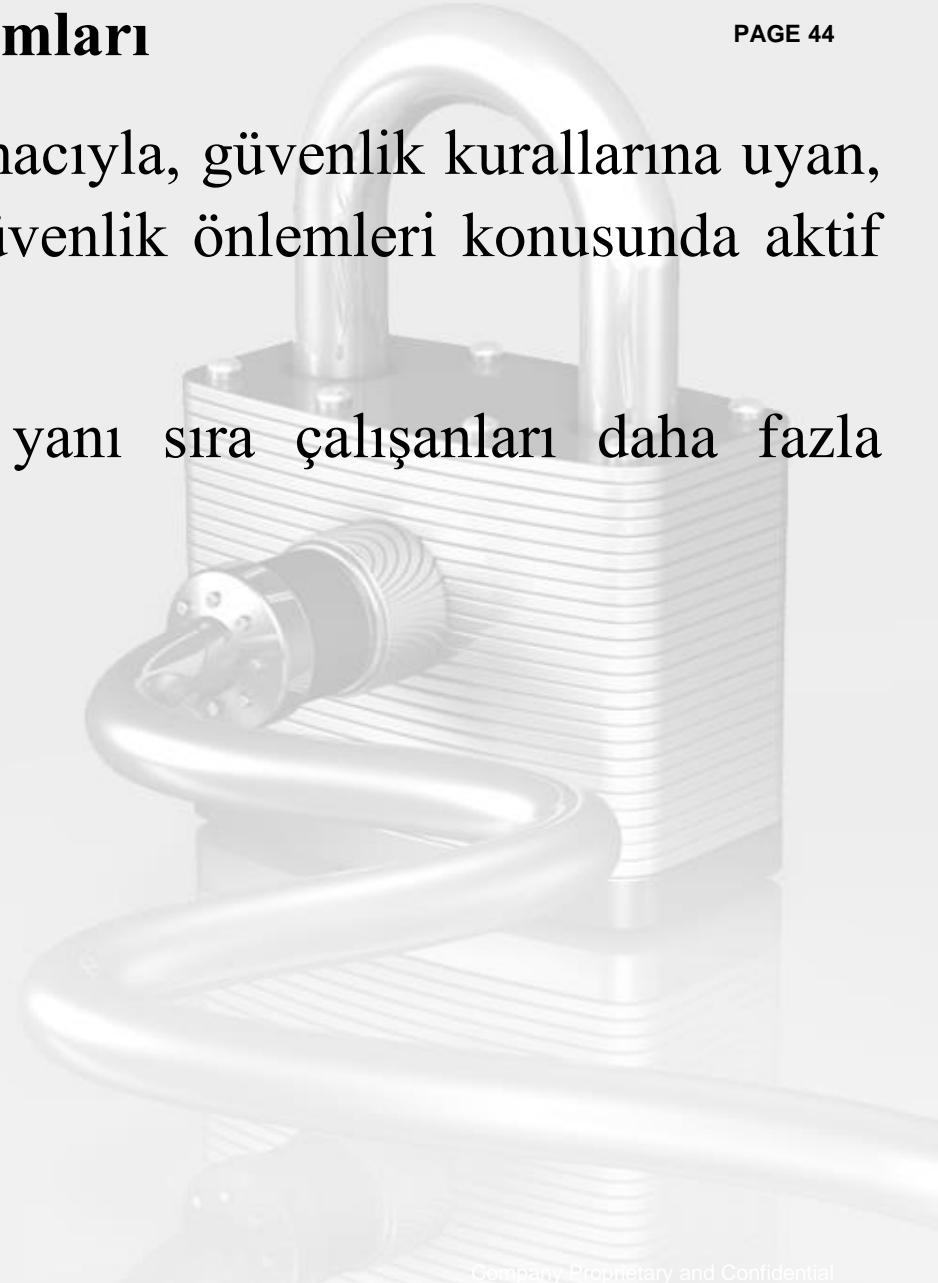
Çalışanların politikaları anlaması ve içselleştirmesi için eğitimler sırasında politikaların önemi vurgulanmalıdır.



## E. Teşvik ve Ödüllendirme Programları

Güvenlik kültürünü teşvik etmek amacıyla, güvenlik kurallarına uyan, güvenlik açıklarını bildiren veya güvenlik önlemleri konusunda aktif olan çalışanlar ödüllendirilebilir.

Bu, güvenlik bilincini artırmanın yanı sıra çalışanları daha fazla katılım sağlamaya teşvik eder.



## **F. Güvenlik Farkındalığının Performans Göstergesi Olarak Belirlenmesi**

Çalışanların bilgi güvenliği bilinci, performans değerlendirmelerinde dikkate alınabilir.

Bu yaklaşım, çalışanların güvenlik konusundaki sorumluluklarını daha ciddiye almalarını sağlar.



# Farkındalık Eğitimleri ve Güvenlik Kültürü Oluşturmanın Faydaları

- 1. İnsan Kaynaklı Riskleri Azaltmak:** İnsan hatasından kaynaklanan güvenlik risklerini en aza indirmek.
- 2. Daha Güçlü Güvenlik Politikaları:** Güvenlik politikalarının çalışanlar tarafından anlaşılıp uygulanmasını sağlamak.
- 3. İhlal Bildiriminin Artması:** Güvenlik kültürü gelişmiş organizasyonlarda, çalışanlar potansiyel tehditleri veya ihlalleri daha hızlı bildirir.

**4. Daha Hızlı ve Etkili Olay Müdahalesi:** Güvenlik kültürü oturmuş çalışanlar, olay anında güvenlik prosedürlerini doğru şekilde uygulayarak hasarı minimize eder.

**5. Yasal Uyumluluk ve Denetimlerin Başarısı:** Güvenlik kültürü, KVKK, GDPR gibi yasal düzenlemelere uyum sürecini kolaylaştırır.



# Farkındalık Eğitimleri ve Güvenlik Kültürü İçin Kullanılabilecek Araçlar ve Yöntemler

- 1. E-Öğrenme Platformları:** Farkındalık eğitimlerinin kolayca ulaşılabilir olması için çevrimiçi eğitim platformları kullanılabilir.
- 2. Siber Saldırı Simülasyonları:** Phishing testleri, sosyal mühendislik senaryoları ve siber saldırı simülasyonları, çalışanların pratik yapmasını sağlar.
- 3. Güvenlik Posterleri ve Hatırlatıcıları:** Güvenlik kültürünü desteklemek için ofis ortamında güvenlik posterleri ve hatırlatıcılar kullanılabilir.



**4. Güvenlik Bültenleri ve Haberleri:** Düzenli olarak yayınlanan güvenlik bültenleri ile çalışanlar, güvenlik tehditleri ve alınması gereken önlemler hakkında bilgilendirilir.

**5. Açık Geri Bildirim ve Destek Kanalları:** Çalışanların güvenlik endişelerini veya şüpheli durumları kolayca bildirebilecekleri bir sistem kurulabilir.

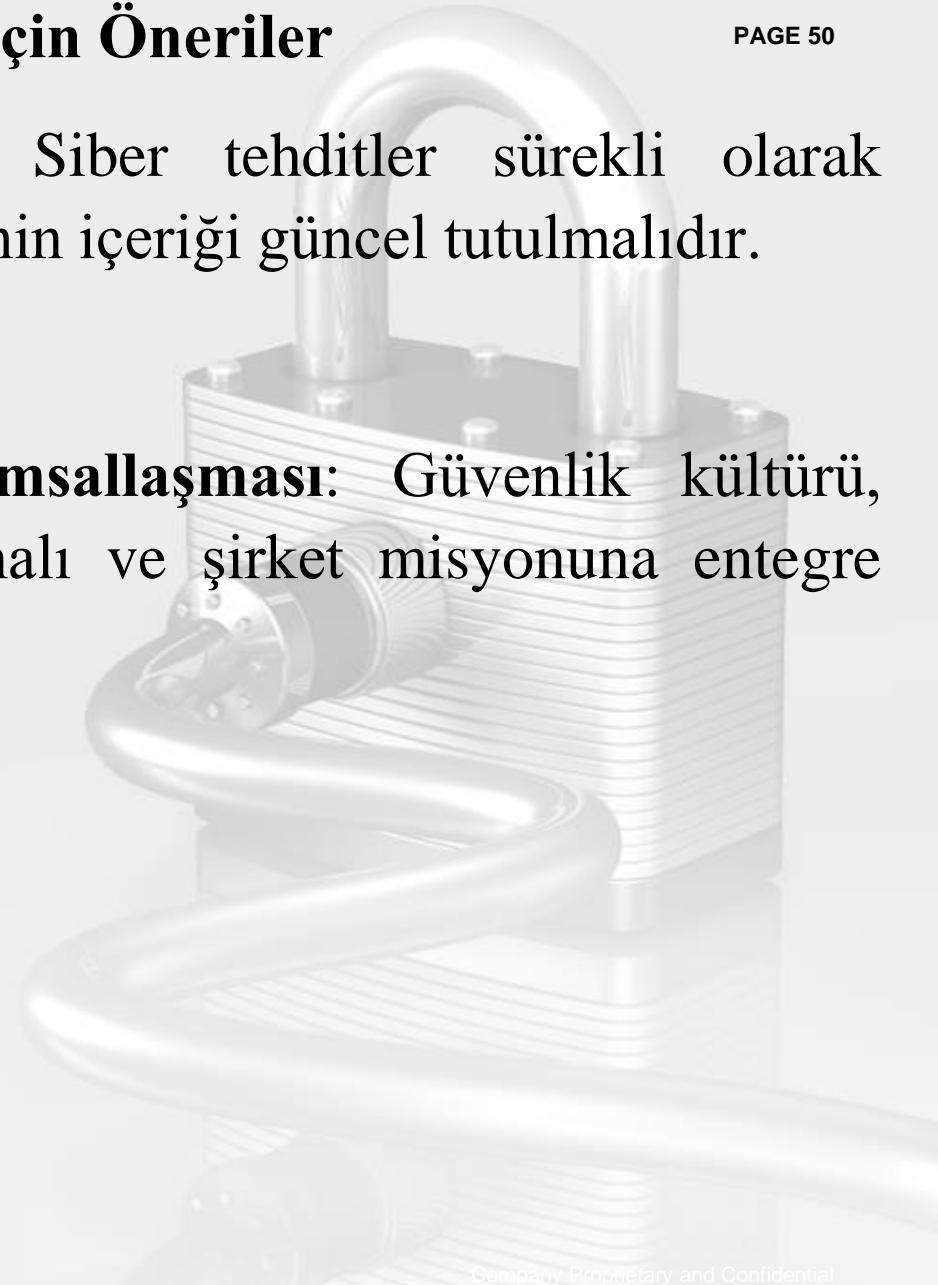


# Güvenlik Kültürünün Sürekliliği İçin Öneriler

PAGE 50

**Eğitimlerin Güncel Tutulması:** Siber tehditler sürekli olarak değiştiğinden, farkındalık eğitimlerinin içeriği güncel tutulmalıdır.

**Eğitimlerin ve Kültürün Kurumsallaşması:** Güvenlik kültürü, şirketin değerleri arasında yer almalı ve şirket misyonuna entegre edilmelidir.



**Geri Bildirim ve Sürekli İyileştirme:** Eğitim programları düzenli olarak değerlendirilip güncellenmeli ve çalışanlardan gelen geri bildirimler dikkate alınmalıdır.

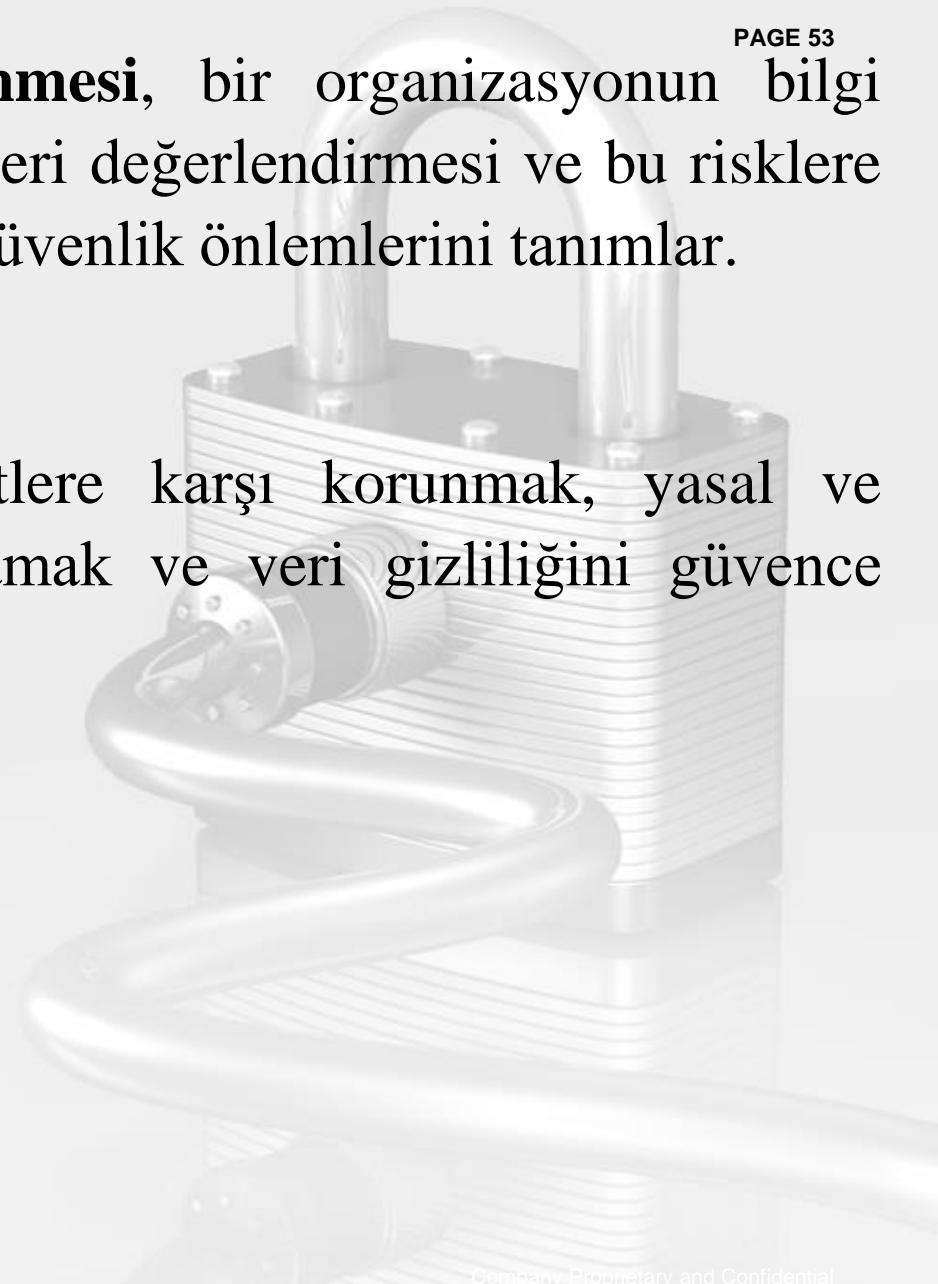
Farkındalık eğitimleri ve güçlü bir güvenlik kültürü, organizasyonların güvenlik duruşunu önemli ölçüde iyileştirir ve bilgi güvenliği tehditlerine karşı direnç kazanmalarını sağlar.

# Güvenlik Kontrollerinin Belirlenmesi



**Güvenlik Kontrollerinin Belirlenmesi**, bir organizasyonun bilgi güvenliğini sağlamak amacıyla riskleri değerlendirmesi ve bu risklere karşı önlem alması için uyguladığı güvenlik önlemlerini tanımlar.

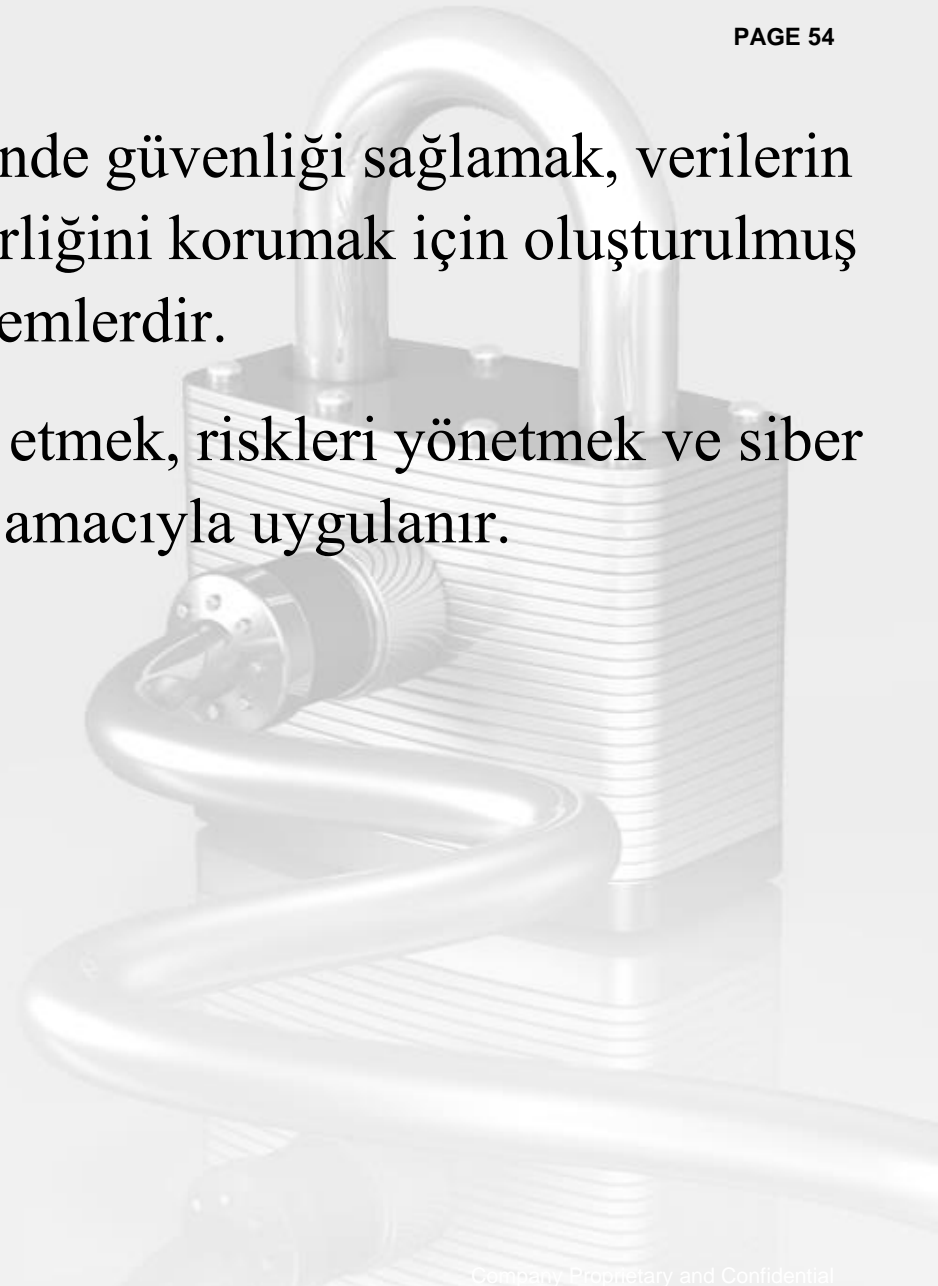
Güvenlik kontrolleri, siber tehditlere karşı korunmak, yasal ve endüstri standartlarına uyum sağlamak ve veri gizliliğini güvence altına almak için geliştirilir.



# Güvenlik Kontrolleri Nedir?

Güvenlik kontrolleri, bilgi sistemlerinde güvenliği sağlamak, verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak için oluşturulmuş prosedürler, politikalar ve teknik önlemlerdir.

Kontroller, güvenlik açıklarını tespit etmek, riskleri yönetmek ve siber tehditlere karşı savunma geliştirmek amacıyla uygulanır.



# Güvenlik Kontrollerinin Türleri

## 1. Fiziksel Güvenlik Kontrolleri:

Fiziksel erişimi sınırlamak için uygulanan güvenlik önlemleridir.

Sunucu odaları, veri merkezleri gibi kritik alanlara erişim için kimlik doğrulama sistemleri, kameralar, biyometrik tarayıcılar ve güvenlik kartları kullanılır.

## 2. Teknik Güvenlik Kontrolleri:

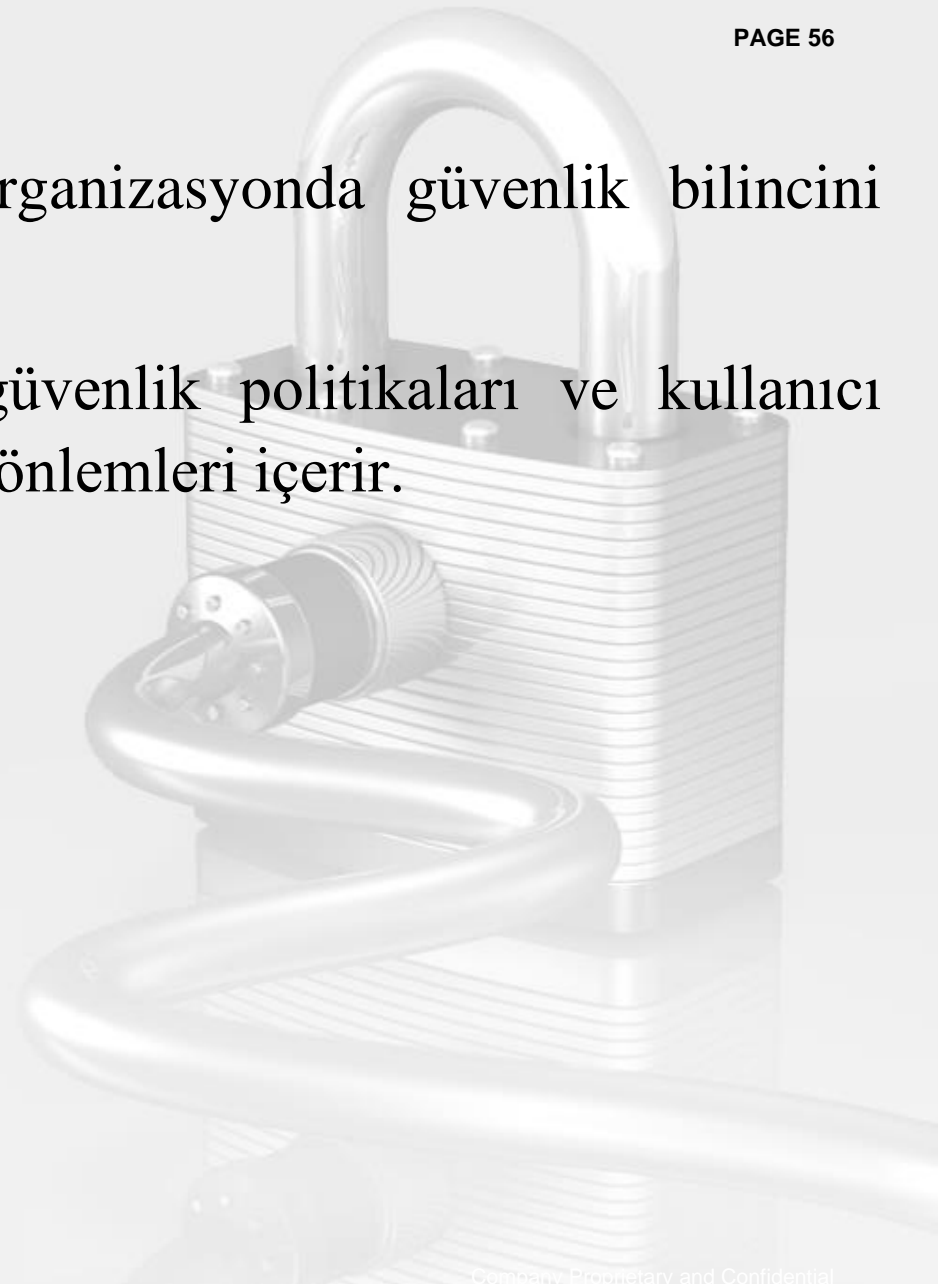
Bilgi teknolojileri altyapısında kullanılan yazılım ve donanımları korumak için uygulanan kontrollerdir.

Bu kontroller, güvenlik duvarları, ağ segmentasyonu, şifreleme, antivirüs yazılımları ve saldırı tespit sistemlerini içerir.

### 3. İdari Güvenlik Kontrolleri:

Politika, prosedür ve kurallarla organizasyonda güvenlik bilincini artırmayı hedefleyen kontrollerdir.

Güvenlik farkındalığı eğitimleri, güvenlik politikaları ve kullanıcı erişim yetkilerinin belirlenmesi gibi önlemleri içerir.



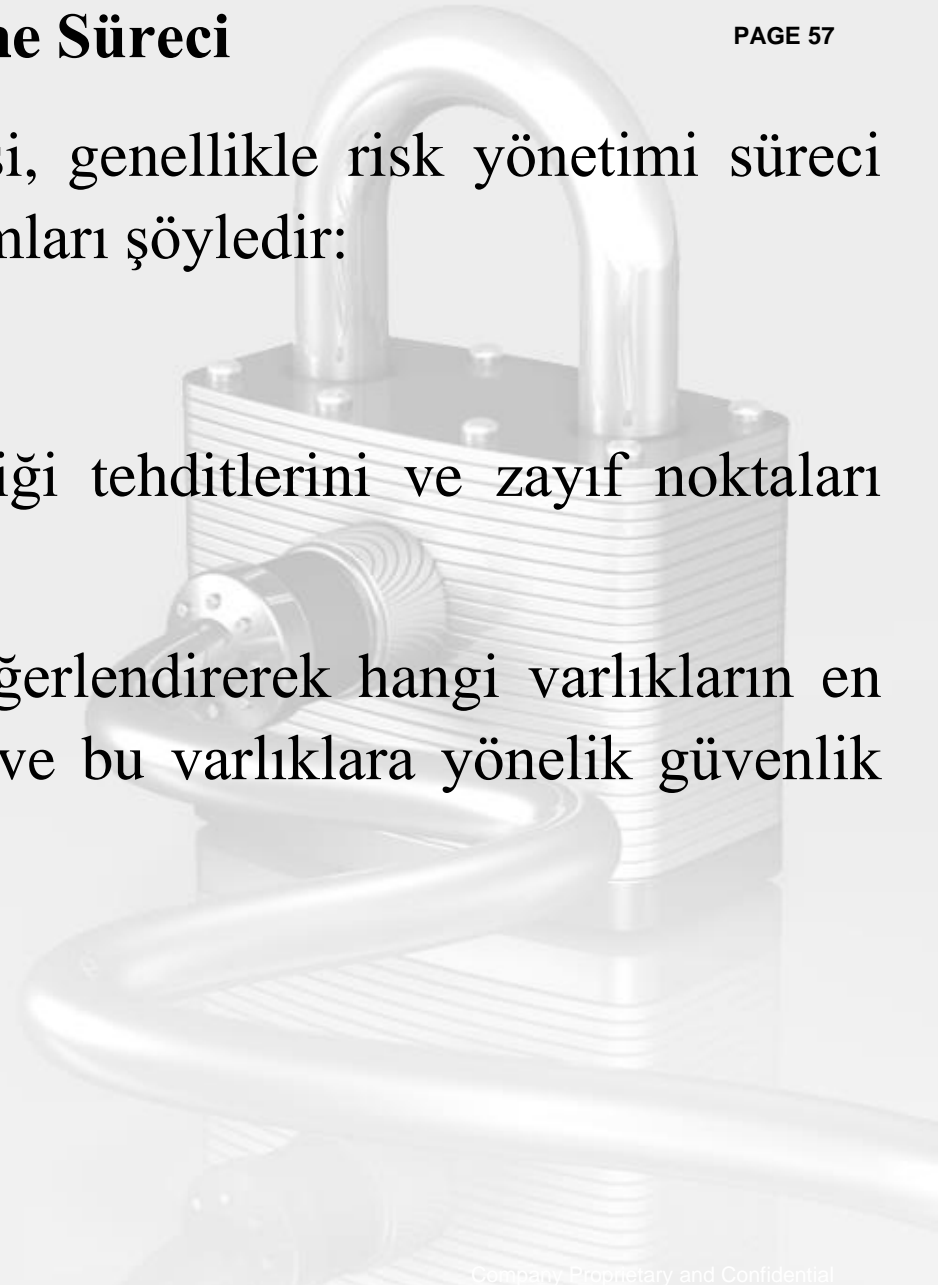


Güvenlik kontrollerinin belirlenmesi, genellikle risk yönetimi süreci çerçevesinde yapılır. Bu sürecin adımları şöyledir:

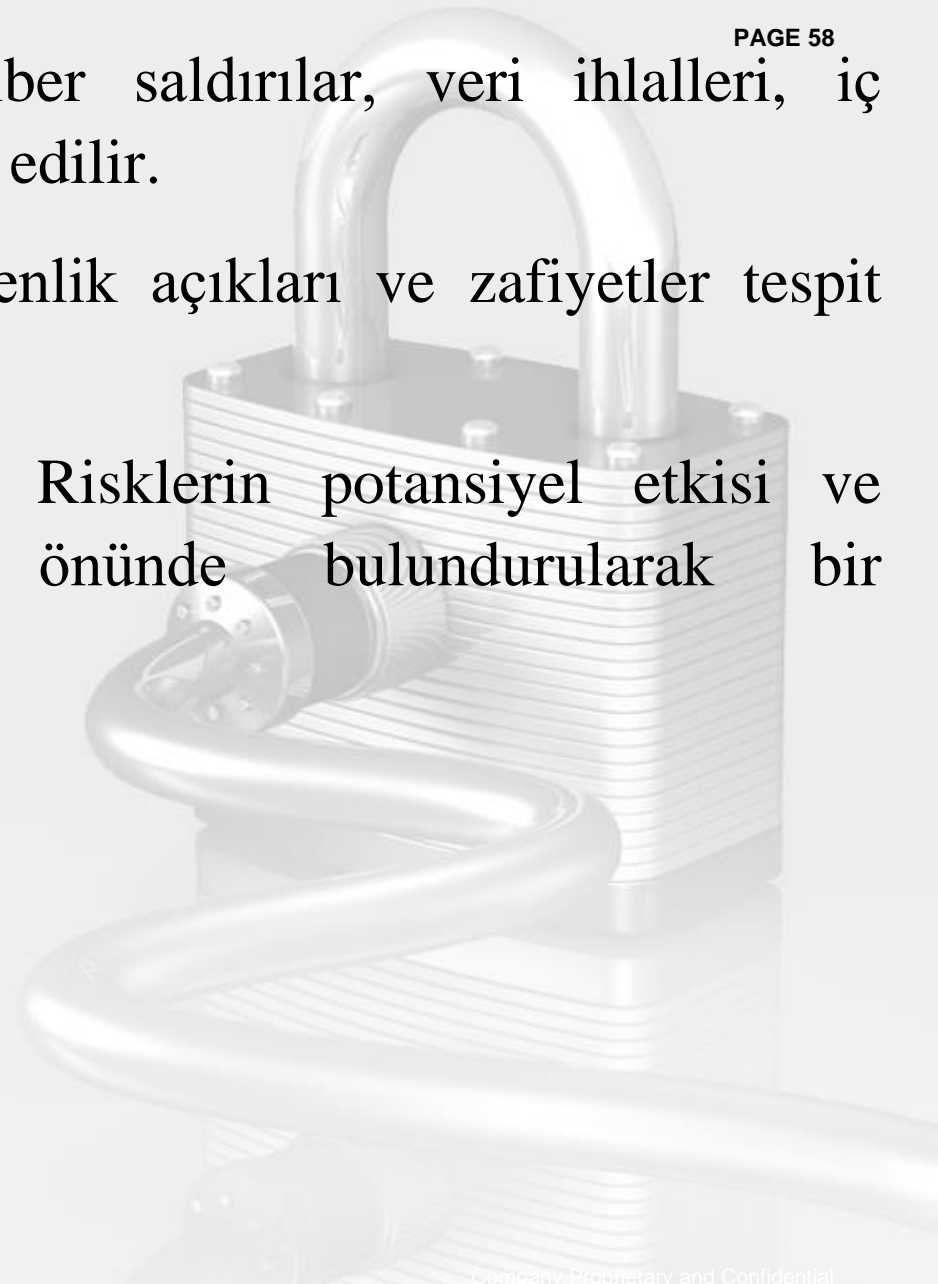
## 1. Risk Değerlendirmesi

Risk değerlendirme, bilgi güvenliği tehditlerini ve zayıf noktaları belirlemek için yapılan bir analizdir.

Organizasyon, bilgi varlıklarını değerlendirerek hangi varlıkların en fazla riske sahip olduğunu belirler ve bu varlıklara yönelik güvenlik açıklarını analiz eder.



- **Tehditlerin Tanımlanması:** Siber saldırılar, veri ihlalleri, iç tehditler gibi olası tehditler analiz edilir.
- **Zafiyetlerin Belirlenmesi:** Güvenlik açıkları ve zafiyetler tespit edilir.
- **Risklerin Önceliklendirilmesi:** Risklerin potansiyel etkisi ve gerçekleşme olasılığı göz önünde bulundurularak bir önceliklendirme yapılır.



## 2. Uygun Güvenlik Kontrollerinin Seçilmesi

PAGE 59.

Risk değerlendirmesinin sonuçlarına göre, riskleri yönetmek için uygun güvenlik kontrolleri seçilir. Bu kontrollerin seçimi, tehditlerin yapısına, riskin büyüklüğüne ve organizasyonun güvenlik gereksinimlerine bağlı olarak yapılır.

- **Önleyici Kontroller:** Tehditlerin gerçekleşmesini engellemeyi amaçlayan kontrollerdir. Örneğin, çok faktörlü kimlik doğrulama (MFA), güvenlik duvarları ve erişim kontrol sistemleri.
- **Tespit Edici Kontroller:** Güvenlik ihlallerini ve anormal olayları hızlıca fark etmek için uygulanan kontrollerdir. Saldırı tespit sistemleri (IDS) ve güvenlik bilgisi ve olay yönetimi (SIEM) sistemleri gibi araçlar kullanılır.
- **Düzeltilici Kontroller:** Güvenlik ihlali sonrasında sistemi eski haline getirmek veya hasarı en aza indirmek için uygulanan kontrollerdir. Yedekleme sistemleri ve felaket kurtarma planları buna örnektir.

### 3. Güvenlik Standartları ve Çerçeveslerinden Faydalanma

PAGE 60

Güvenlik kontrollerinin belirlenmesi sürecinde, organizasyonlar uluslararası standartlardan ve güvenlik çerçevelerinden yararlanır. En sık kullanılan standartlardan bazıları şunlardır:

- **ISO/IEC 27001:** Bilgi güvenliği yönetim sistemi (BGYS) standartlarını belirler ve güvenlik kontrollerinin sistematik bir yapıda uygulanmasını sağlar.
- **NIST (National Institute of Standards and Technology):** NIST'in 800-53 çerçevesi, bilgi güvenliği için detaylı güvenlik kontrolleri sunar.
- **CIS (Center for Internet Security) Kontrolleri:** Siber tehditlere karşı en iyi güvenlik önlemlerini tanımlar.
- **COBIT (Control Objectives for Information and Related Technologies):** Bilgi teknolojisi süreçlerinin yönetimi için güvenlik kontrolleri sağlar.

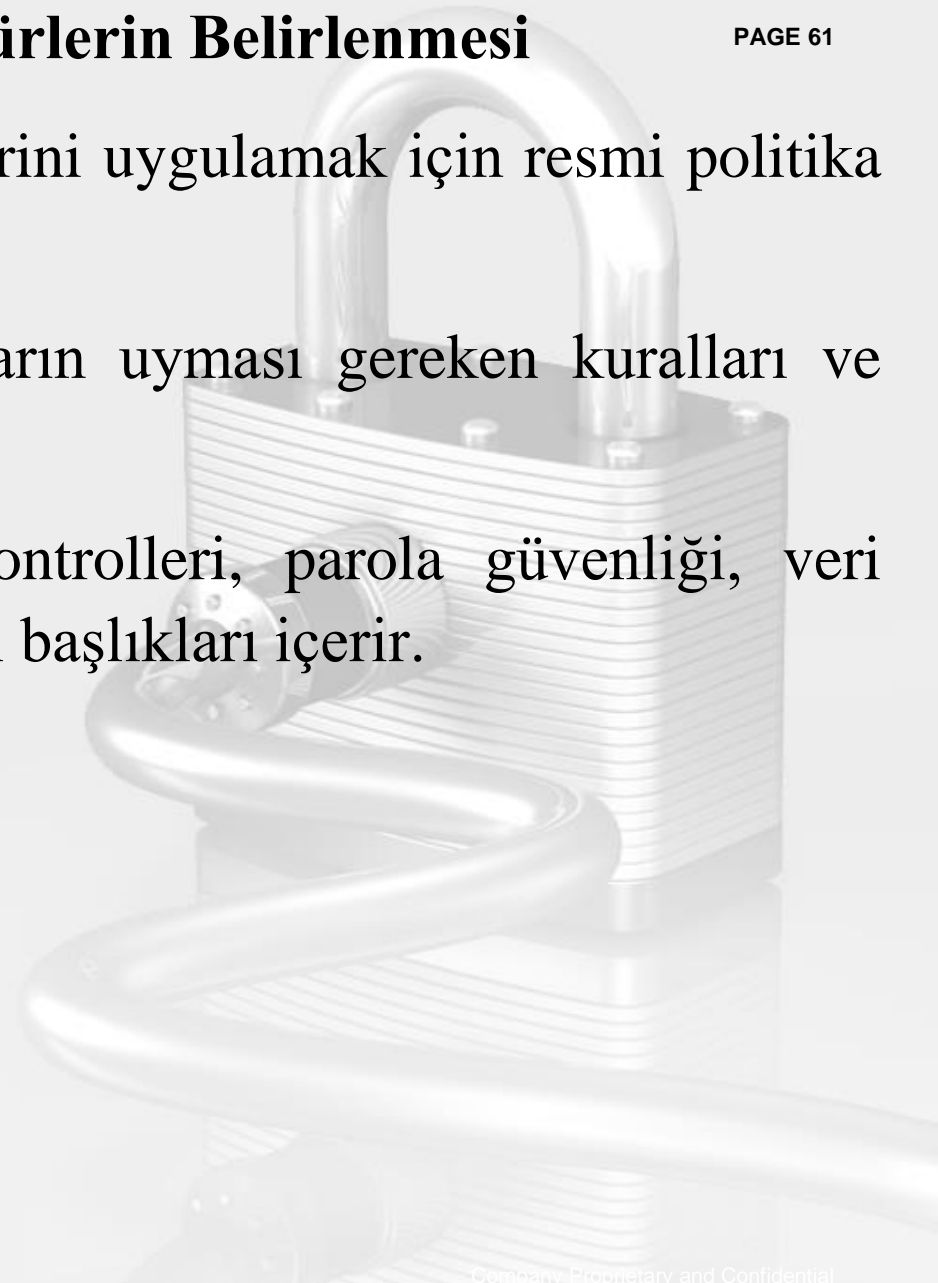
## 4. Güvenlik Politikaları ve Prosedürlerin Belirlenmesi

PAGE 61

Organizasyonlar, güvenlik kontrollerini uygulamak için resmi politika ve prosedürler geliştirir.

Güvenlik politikaları, tüm çalışanların uyması gereken kuralları ve güvenlik uygulamalarını açıklar.

Bu politikalar, kullanıcı erişim kontrolleri, parola güvenliği, veri koruma, yedekleme prosedürleri gibi başlıkları içerir.



## 5. Güvenlik Kontrollerinin Uygulanması ve Test Edilmesi

Belirlenen güvenlik kontrolleri, uygulama aşamasında titizlikle test edilir ve değerlendirilir. Bu aşamada güvenlik kontrollerinin işlevselliği test edilir ve eksiklikler belirlenerek düzeltilir.

- **Penetrasyon Testleri:** Güvenlik kontrollerinin etkinliğini değerlendirmek için saldırı simülasyonları yapılır.
- **Zafiyet Taramaları:** Güvenlik açıklarını düzenli olarak taramak ve yeni açıkları hızla tespit etmek için kullanılan araçlardır.

## 6. İzleme ve Sürekli İyileştirme

Uygulanan güvenlik kontrollerinin etkili olup olmadığını değerlendirmek ve güvenlik durumunu sürekli iyileştirmek için kontrollerin izlenmesi gerekir. Bu süreç, BT güvenlik ekipleri tarafından sürekli izleme, raporlama ve değerlendirme ile yürütülür.

- **Olay Yönetimi ve Kayıt Tutma:** Güvenlik olayları kayıt altına alınır ve analiz edilir.
- **Güvenlik Kontrollerinin Güncellenmesi:** Tehdit ortamındaki değişikliklere göre kontrollerin güncellenmesi gerekebilir.

- 1. Güvenlik Risklerinin Azaltılması:** Güvenlik kontrolleri, bilgi güvenliği risklerini minimize ederek bilgi varlıklarının daha güvenli olmasını sağlar.
- 2. Yasal Uyumluluk:** KVKK, GDPR gibi yasal düzenlemelere uyum sağlamak için güvenlik kontrolleri zorunludur.
- 3. Veri Gizliliği ve Güvenliği Sağlama:** Güvenlik kontrolleri, veri gizliliğini ve güvenliğini sağlayarak müşteri ve kullanıcı verilerinin korunmasına yardımcı olur.
- 4. Siber Tehditlere Karşı Koruma:** Güvenlik kontrolleri, organizasyonu siber tehditlere karşı koruyarak güvenlik ihlallerini engeller.
- 5. Olay Müdahale Hızının Artırılması:** Güvenlik kontrolleri, güvenlik olaylarını tespit etmeyi ve hızla müdahale etmeyi sağlar.



**Özetle,** Güvenlik kontrollerinin belirlenmesi, organizasyonun bilgi güvenliği politikalarının temel taşlarından biridir.

Bu kontrollerin uygulanması, hem organizasyonun yasal uyumunu sağlar hem de veri güvenliğini üst seviyeye çıkarır.

Güvenlik kontrolleri düzenli olarak gözden geçirilmeli, test edilmeli ve değişen tehditlere göre sürekli iyileştirilmelidir.

Bu, organizasyonun siber güvenlikte güçlü bir konuma sahip olmasını ve karşılaşılabileceği tehditlere karşı daha dayanıklı olmasını sağlar.

# **Güvenlik Politikalarının Oluşturulması ve Güvenlik Standartları**



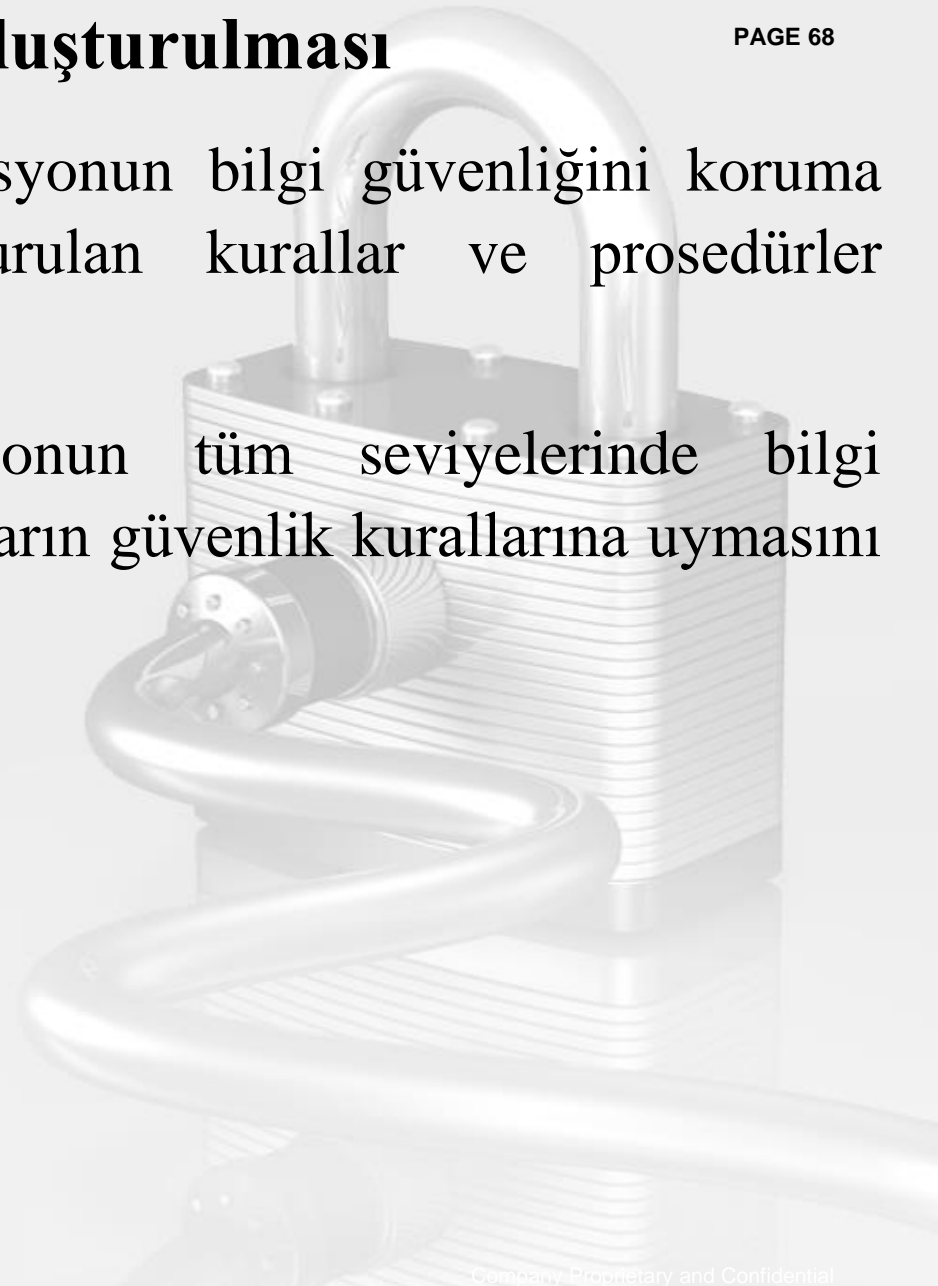
**Güvenlik Politikalarının Oluşturulması ve Güvenlik Standartları,** organizasyonların bilgi güvenliği yönetim stratejilerinin temelini oluşturur.

Güvenlik politikaları, organizasyonun bilgi güvenliği hedeflerine ulaşmak için izlediği kurallar ve uygulamaları belirlerken; güvenlik standartları, bilgi güvenliğini sağlamak için en iyi uygulama rehberleri sunar

# 1. Güvenlik Politikalarının Oluřturulması

Güvenlik politikaları, bir organizasyonun bilgi güvenliğini koruma hedeflerine ulaşması için oluşturulan kurallar ve prosedürler bütünüdür.

Güvenlik politikaları, organizasyonun tüm seviyelerinde bilgi güvenliği bilincini artırır ve çalışanların güvenlik kurallarına uymasını sağlar.



- **Bilgi Güvenliğini Sağlamak:** Bilgi varlıklarını yetkisiz erişim, veri ihlalleri ve siber saldırılardan korumak.
- **Risk Yönetimini Desteklemek:** Riskleri azaltarak güvenlik ihlallerini önlemek.
- **Yasal Uyumluluk:** KVKK, GDPR gibi yasal düzenlemelere uyum sağlamak.
- **Kurum İçi Güvenlik Bilincini Artırmak:** Çalışanların güvenlik konularında farkındalığını artırmak ve güvenlik kültürü oluşturmak.

Güvenlik politikaları, organizasyonun bilgi güvenliği ihtiyaçlarına göre farklı başlıklar altında oluşturulabilir:

- 1. Bilgi Güvenliği Politikası:** Organizasyonun bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için temel güvenlik ilkelerini içerir.
- 2. Erişim Kontrol Politikası:** Sadece yetkilendirilmiş kişilerin bilgi varlıklarına erişebilmesi için kullanıcı yetkilendirmesi ve kimlik doğrulama kurallarını belirler.

**3. Yedekleme ve Felaket Kurtarma Politikası:** Veri kaybını önlemek için verilerin düzenli olarak yedeklenmesini ve beklenmedik bir olay durumunda verilerin geri yüklenmesi için felaket kurtarma prosedürlerini kapsar.

**4. Mobil Cihaz Güvenliği Politikası:** Çalışanların organizasyon verilerine mobil cihazlar üzerinden erişimi için güvenlik önlemlerini tanımlar.

**5. Şifreleme ve Veri Koruma Politikası:** Hassas verilerin şifrelenerek korunması için kullanılan teknikleri ve prosedürleri belirler.

- 1. Risk Analizi:** İlk adım, organizasyonun bilgi güvenliği risklerini belirlemek ve bu riskleri en aza indirmek için politikalar oluşturmaktır.
- 2. Politika Taslağının Hazırlanması:** Güvenlik gereksinimlerine ve risk analizine dayanarak, bilgi güvenliği politikasının taslağı hazırlanır. Taslak, erişim kontrolü, şifreleme, veri yedekleme gibi başlıkları kapsar.



**3. Yönetimin Onayı:** Hazırlanan güvenlik politikası taslağı, yönetim tarafından onaylanarak resmi olarak organizasyon politikasına dahil edilir.

**4. Çalışanlara Duyuru ve Eğitim:** Güvenlik politikalarının tüm çalışanlara duyurulması ve bu politikalar hakkında farkındalık eğitimi verilmesi gereklidir.

**5. Politikanın Sürekli Gözden Geçirilmesi ve Güncellenmesi:** Güvenlik tehditleri, teknoloji ve yasal düzenlemeler zaman içinde değişiklik gösterir. Bu nedenle güvenlik politikaları, düzenli olarak gözden geçirilerek güncellenmelidir.

## 2. Güvenlik Standartları

Güvenlik standartları, bilgi güvenliği yönetimi için küresel olarak kabul edilmiş en iyi uygulamaları sunar. Bu standartlar, organizasyonların güvenlik politikalarını oluşturmada ve uygulamalarında rehberlik eder.

### **ISO 27001 – Bilgi Güvenliği Yönetim Sistemi (BGYS)**

- ISO 27001, Uluslararası Standardizasyon Örgütü tarafından yayımlanan bir bilgi güvenliği yönetim sistemi (BGYS) standardıdır.

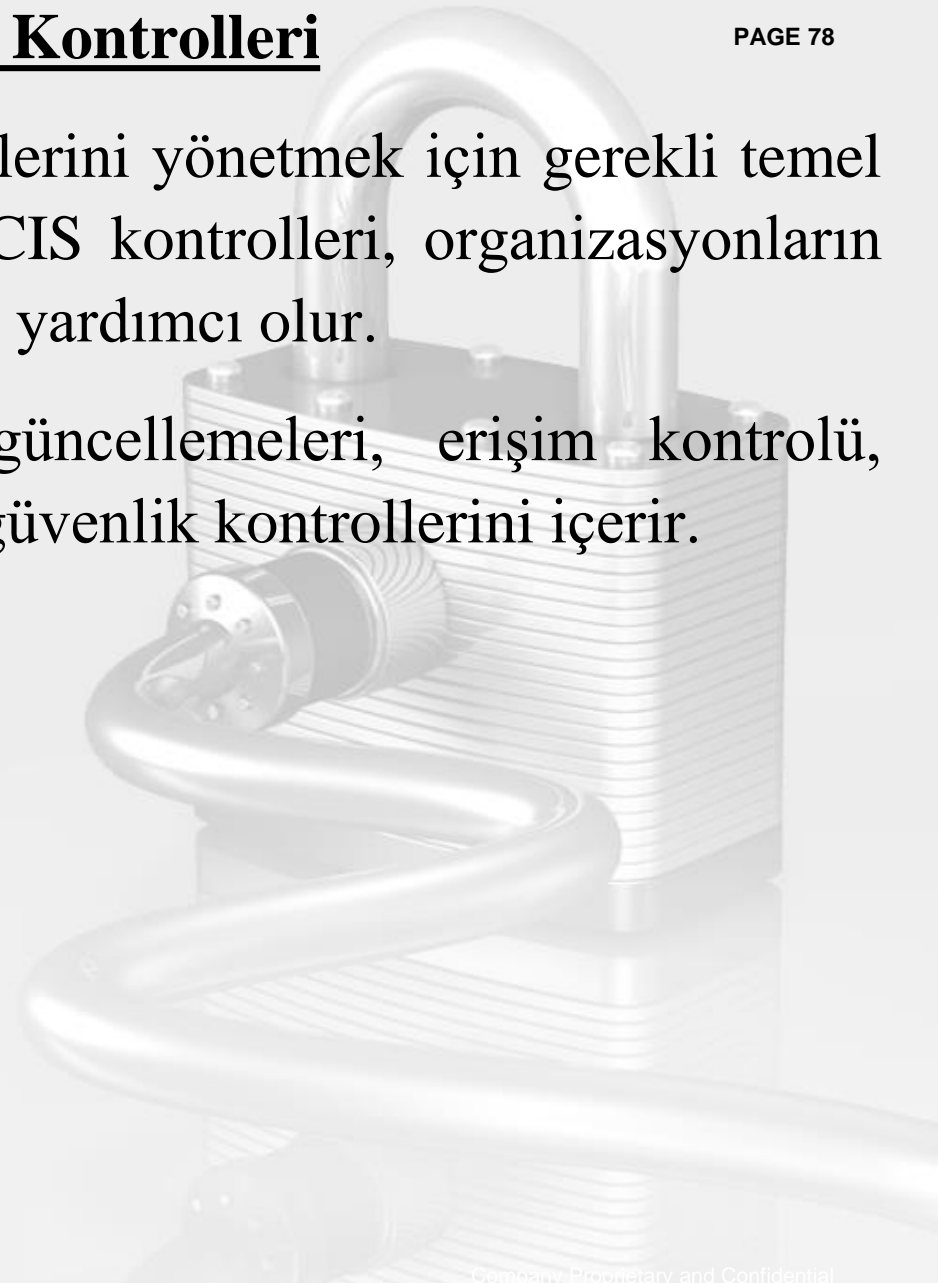
- ISO 27001, bilgi güvenliği yönetiminin yapılandırılmasını, uygulanmasını, izlenmesini ve sürekli iyileştirilmesini sağlar.
- **Risk Yönetimi:** ISO 27001, bilgi güvenliği risklerinin tanımlanması, değerlendirilmesi ve riskleri azaltmak için uygun güvenlik kontrollerinin uygulanmasını içerir.
- **Uyumluluk ve Sertifikasyon:** ISO 27001'e uyumlu olmak, bir organizasyonun güvenlik uygulamalarının uluslararası standartlara uygun olduğunu gösterir. Sertifikasyon almak için bağımsız denetimlerden geçmek gereklidir.

- NIST, Amerika Birleşik Devletleri'nde federal kurumlar için güvenlik rehberliği sağlayan bir standart geliştirmiştir. Özellikle NIST 800 serisi, bilgi güvenliği kontrolleri ve risk yönetimi konusunda ayrıntılı rehber sunar.
- NIST çerçevesi, risk değerlendirmesi, erişim kontrolü, güvenlik testleri, olay yönetimi gibi geniş bir güvenlik kontrol yelpazesini içerir.
- **NIST 800-53:** NIST 800-53, bilgi güvenliği kontrolleri konusunda ayrıntılı bir rehberdir. Kamu sektöründe sıkça kullanılsa da özel sektörde de yaygın olarak tercih edilmektedir.

# **COBIT (Control Objectives for Information and Related Technologies)**

- COBIT, bilgi teknolojileri yönetimi ve denetim çerçevesidir ve bilgi güvenliği yönetimi, BT varlıklarının yönetimi gibi konuları içerir.
- COBIT, güvenlik hedeflerine ulaşmak için BT süreçlerinin nasıl yönetilmesi gerektiğini açıklar. Özellikle büyük ölçekli organizasyonlarda BT yönetimini kolaylaştırmak için kullanılır.

- CIS, en kritik siber güvenlik risklerini yönetmek için gerekli temel güvenlik kontrollerini tanımlar. CIS kontrolleri, organizasyonların siber tehditlere karşı korunmasına yardımcı olur.
- Güvenlik denetimi, güvenlik güncellemeleri, erişim kontrolü, şifreleme, yedekleme gibi pratik güvenlik kontrollerini içerir.



# **Uyum ve Düzenlemeler**

## **(KVKK, GDPR Yasal Düzenlemeler)**

Organizasyonlar, güvenlik politikalarını oluştururken, yürürlükteki yasal düzenlemelere uyum sağlamak zorundadır. Bu yasal düzenlemeler, veri gizliliği ve güvenliği konusunda temel çerçeveyi sunar.

### **KVKK (Kişisel Verilerin Korunması Kanunu)**

- Türkiye’de yürürlükte olan KVKK, kişisel verilerin korunması için oluşturulmuş bir yasal düzenlemedir. Organizasyonların, kişisel verilerin güvenliğini sağlamak amacıyla güvenlik politikaları oluşturmasını zorunlu kılar.

**Gereksinimler:** Kişisel verilerin işlenmesi, saklanması, üçüncü taraflarla paylaşılması gibi konularda güvenlik önlemleri almayı zorunlu kılar.



# **GDPR (General Data Protection Regulation)**

- Avrupa Birliği'nde geçerli olan GDPR, bireylerin kişisel verilerini koruma amacıyla oluşturulmuş bir yasal düzenlemedir.

**Gereksinimler:** Kişisel veri işleme prosedürlerini ve veri ihlali durumunda organizasyonların yapması gerekenleri ayrıntılı olarak belirler. Ciddi ihlaller durumunda organizasyonlar için yüksek para cezaları öngörülmektedir.

**Not:** Güvenlik politikalarının oluşturulması ve güvenlik standartlarına uyum, organizasyonun bilgi güvenliğini sağlama yolundaki temel adımlardır.

Güvenlik politikaları, çalışanların güvenlik kurallarına uymasını sağlarken; güvenlik standartları, güvenlik risklerini azaltmak ve tehditlere karşı savunma sağlamak için bir rehber işlevi görür.

Bu politikaların ve standartların belirli aralıklarla gözden geçirilmesi, organizasyonun sürekli olarak güvenliğini artırmasını ve siber tehditlere karşı korunmasını sağlar.

Gelecek Dersimizde;

PAGE 83

## Uygulama Geliştirme Güvenliđi

