



## Bilgi Güvenliđi Politikası

Doküman No

POL.BS.01

Doküman Sahibi

Bilgi Sistemleri Yöneticiliđi

Revizyon No	Revizyon Tarihi	Revizyon Tanımı	Revizyonu Yapan	Onaylayan
0	19.10.2018	İlk Yayın	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
1	17.09.2021	ISO/IEC 27001:2017 standardı eklendi.	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
2	22.11.2021	Bilgi güvenliđi hedeflerine tedarikçi bilgi güvenliđi ifadesi eklendi.	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
2	10.08.2022	Güncelliđi gözden geçirildi.	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
3	15.03.2023	Güncelliđi gözden geçirildi ve imla hataları düzeltildi.	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
4	29.11.2023	3.Tanımlar, Roller, Sorumluluklar ve Yetkiler başliđı, 3. Tanımlar, 4 Roller Sorumluluklar ve Yetkiler olarak ayrıldı. Roller, Sorumluluklar ve Yetkiler başliđı detaylandırıldı. 5 Politika başliđı ve altındaki alt başlıklar güncellendi. 6 Politikanın Gelişimi altındaki ibareler düzenlendi.	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu
5	04.04.2024	Doküman şablonu, Dokümanların Kontrolü Prosedürüne göre uygun yazı tipi vb. formata göre düzenledi. 5.2 Bilgi Güvenliđi Politikası	Bilgi Güvenliđi Yöneticisi	Yönetim Kurulu

Hazırlayan


Bilgi Güvenliđi Yöneticisi

Kontrol Eden

Bilgi Güvenliđi Yönetim  
Temsilcisi - Üst Yönetim


Onaylayan

Yönetim Kurulu

	<b>Bilgi Güvenliđi Politikası</b>	
	Doküman No	POL.BS.01
	Doküman Sahibi	Bilgi Sistemleri Yöneticiliđi

		<i>başlıđının altındaki ibareler güncellendi. 6 Politikanın Gelişimi başlıđının altındaki ibareler düzenledi.</i>		
6	08.01.2025	<i>Onay mekanizmaları revize edildi.</i>	<i>Bilgi Güvenliđi Yöneticisi</i>	<i>Yönetim Kurulu</i>
6	06.04.2026	<i>Güncelliđi gözden geçirildi.</i>	<i>Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim</i>	<i>Yönetim Kurulu</i>

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
Bilgi Güvenliđi Yöneticisi	Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim	Yönetim Kurulu

	<b>Bilgi Güvenliđi Politikası</b>	
	<b>Doküman No</b>	<b>POL.BS.01</b>
	<b>Doküman Sahibi</b>	<b>Bilgi Sistemleri Yöneticiliđi</b>

### 1. Amaç

Bu politikanın amacı, hukuka, yasal düzenleyici ya da sözleşmeye tabi yükümlülöklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, Üst Yönetim'in bilgi güvenliđi yaklaşımını tanımlamak, tüm çalışanlara ve ilgili taraflara bildirmektir.

Bilgi Güvenliđi Politikası kurumsal bilgi güvenliđi ilkelerimizi ana hatlarıyla belirler. Bilgi Güvenliđi Politikası, kurumda bilginin ve işleme yöntemlerinin güvenli olarak gerçekleştirilmesi amacıyla düzenlemeler yapar.

### 2. Kapsam

Bu politika Bilgi Güvenliđi Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları, ve diđer tüm paydaşlara ilişkin süreçleri kapsamaktadır.

### 3. Tanımlar

**Bilgi Güvenliđi Yönetim Sistemi (BGYS):** Bilgi güvenliđini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır.

**Bilgi Varlığı:** Şirket'in sahip olduđu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduđu bilgi sistemleri varlıklarıdır.

**Gizlilik:** Bilginin yetkisiz kişilerin eline geçmesini önlemek ve yetkisiz erişime karşı korumaktır.

**Bütünlük:** Bilginin yetkisiz kişiler tarafından deđiştirilmesini engellemek ve bilginin doğruluđunu sağlamaktır.

**Erişilebilirlik:** Bilginin yetkili kişiler tarafından ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasını sağlamaktır.

**Fikri Mülkiyet Hakları (Intellectual Property Rights):** Bireylerin veya kuruluşların fikir ve yaratıcılık sonucu ortaya çıkan ürünler üzerinde sahip oldukları haklardır.

### 4. Roller Sorumluluklar ve Yetkiler

Bu politikanın hazırlanması, gerekli analizlerin yapılması gözden geçirilmesi, güncellenmesi ve yürürlükten kalkanların toplanarak imha edilmesinden Bilgi Güvenliđi Yöneticisi, kontrol edilmesinden Bilgi Güvenliđi Yönetim Temsilcisi – Üst Yönetim, onaylanmasından Yönetim Kurulu sorumludur.

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliđi Yöneticisi tarafından gözden geçirilir. Arena Bilgisayar Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetimi Bilgi Güvenliđi Politikası'nın tüm çalışanlara ve ilgili diđer tüm paydaşlara duyurulmasını sağlar.


Gözden geçirmeler sonrasında gerçekleştirilen deđişiklikler için Yönetim Kurulu onayı alınır.

### 5. Uygulama

#### 5.1. Yönetim Kurulu Bađlılıđı

Şirket Yönetim Kurulu bilgi güvenliđinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gerekenin yapılacağını taahhüt eder.

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
<b>Bilgi Güvenliđi Yöneticisi</b>	<b>Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim</b>	<b>Yönetim Kurulu</b>

	<b>Bilgi Güvenliđi Politikası</b>	
	<b>Doküman No</b>	<b>POL.BS.01</b>
	<b>Doküman Sahibi</b>	<b>Bilgi Sistemleri Yöneticiliđi</b>

### 5.2. Bilgi Güvenliđi Politikası

- Bilgi Güvenliđi Yönetim Sistemini, uluslararası olarak kabul edilmiş olan TS EN ISO/IEC 27001:2022 Bilgi Güvenliđi Yönetim Sistemi standardı şartları doğrultusunda planlamak, gerçekleştirmek ve geliştirmek.
- Bilgi güvenliđini etkin biçimde yönetmek ve yaşanabilecek olan zararları en aza indirmek ve sürekli iyileştirmesini sağlamak.
- Bilgi güvenliđi ihlallerinin önüne geçmek ve oluşabilecek bilgi güvenliđi ihlallerine koordineli bir şekilde yanıtlamak ve çözüm bulmak.
- İş sürekliliđi kapsamında yaşanabilecek kesintiler için önlem almak ve önüne geçmek.
- Kritik iş süreçlerinin hedef kurtarma süreleri içerisinde, tekrar çalışır hale getirmek.
- Bilgi güvenliđi kapsamındaki yasal yükümlülöklere uyumlu hale gelmek.
- Bilgi Güvenliđi Yönetim Sistemi kapsamında tüm paydaşlarımızın (müşteri, tedarikçi vb.) bilgi varlıklarının gizliliđini, bütünlüğünü ve erişilebilirliğini sağlamak.

### 5.3. Bilgi Güvenliđi Yönetim Sistemleri Genel Süreçleri

Şirket bilgi güvenliđini sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipleri oluşturur. Bilgi Güvenliđi Politikasının belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Bilgi Güvenliđi Yöneticisi desteđi ve tüm birimlerin koordinasyonu ile gerçekleştirilir. Arena Bilgisayar gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.

Bu çerçevede şirket aşağıdaki uygulamalar ile Bilgi Güvenliđi Politikasını benimser ve sistemin işleyişini sürekli hale getirir;

**Varlıklar:** Şirket sahip olduđu bilgi varlıklarını kategorize eder. Bilgi varlığı kategorizasyonunun nasıl yapıldığı ve bilgi varlıklarına nasıl değer ataması yapıldığı Varlık Yönetimi Prosedüründe detaylı olarak anlatılmaktadır.


**Risk Deđerlendirme ve Risk Analizi:** Bilgi varlıklarıyla ilgili oluşabilecek risklerin belirlenmesi ve risklerin ölçümlenmesi ve deđerlemesinin yapıldığı devamlı bir süreçtir.

**Talimatlar:** Bilgi sistemin uygun şekilde işletilebilmesi, işletmenin genel kurallara bađlı, denetlenebilir, tekrar edilebilir ve iyileştirilebilir olması amacıyla gerekli talimatlar hazırlanır.

**Fikri Mülkiyet Hakları:** Şirket, fikri mülkiyet hakkı taşıyan ürün, yazılım, hizmet veya sistemler sahibinden izin alınmadan veya kullanım lisansı olmadan kullanılamaz.

**Eđitim:** Tüm personele ve gereken durumlarda tüm paydaşlara bilgi güvenliđi farkındalık eğitimi verilmektedir. Eğitim içeriğinde, bilgi güvenliđi ile ilgili politika, prosedür, talimat vb. süreçler anlatılmaktadır. Eğitim kapsamına giren kurallar bütününde muhtemel deđişiklik ve güncellemeler gerçekleştikten sonra bilgi güvenliđi farkındalık eğitimleri tekrarlanır.

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
<b>Bilgi Güvenliđi Yöneticisi</b>	<b>Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim</b>	<b>Yönetim Kurulu</b>

	<b>Bilgi Güvenliđi Politikası</b>	
	<b>Doküman No</b>	<b>POL.BS.01</b>
	<b>Doküman Sahibi</b>	<b>Bilgi Sistemleri Yöneticiliđi</b>

**Yasal Uyumluluk:** Şirket, bilgi güvenliđi ile ilgili yayınlanmış kanun, yönetmelik ve tebliđlere uygun olarak hizmet vermek için gerekli tüm çalıřmaları yapar.

**İř Sürekliliđi:** Üst Yönetim, bilgi güvenliđi iş süreklilik ilkelerini belirler ve iş süreklilik ilkelerinin hayata geçirilmesi için bir İş Süreklilik Planı oluşturulmasını ve deđişen koşullara göre güncel tutulmasını sağlar. Güncel İş Sürekliliđi Planı ile ilgili roller ve sorumluluklar İş Sürekliliđi Planı'nda belirtilir. İş sürekliliđine ilişkin genel prensipler İş Sürekliliđi Politikasında yer almaktadır.


**Temiz Masa Temiz Ekran:** Çalıřma saatleri süresince ve dışında, çalıřanların açık olan bilgisayarlarının veya çalıřma masalarının başından geçici veya sürekli olarak ayrılması gerektiğinde bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar, kaldırılabilir depolama ortamları ve kişisel bilgisayarlar için gerekli şartlara uyulması gerektiđini tanımlamaktadır.

**Sürekli iyileřtirme:** Şirket, bilgi güvenliđi politikasını, denetim sonuçlarını, izlenen bilgi güvenliđi olaylarının analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak Bilgi Güvenliđi Yönetim Sistemini sürekli olarak iyileřtirir.

**Bilgi Güvenliđi Organizasyonu:** Bilgi Güvenliđi Yönetim Sistemi kapsamında organizasyon belirlenmesi ve uygulanması Üst Yönetim sorumluluđundadır. Bu sorumlukların neler olduđu, kişi isimleri ve sorumlulukları BGYS Roller ve Sorumluluklar Prosedürü dokümanında detaylı olarak aktarılmaktadır. Bu dokümanda belirtilen hususlara uyulması ve uygun çalıřılması tüm personeli kapsamaktadır.

- Varlıkların güvenliđini sağlanmasından ve gözetilmesinden tüm personel sorumludur.
- Varlıklara ve bilgilere erişirken Bilgi güvenliđi kapsamında belirlenmiş olan erişim yetki esaslarına uyum konusunda tüm çalıřanlar yükümlüdür.
- Bilgi güvenliđi kontrol önlemlerinin uygulamaya alınması ve kontrolü BGYS Kurulu tarafından gerçekleştirilir.
- Bilgi bulunan her türlü ortamın (elektronik ortam, basılı doküman, usb...vb) saklanması, oluşturulması, imha edilmesi ve erişilmesi konularında belirtilen kurallara uyulması tüm personelin yükümlülüđüdür.
- Bilgi güvenliđi ile ilgili kritik kararların alınması, onaylanması ve gözden geçirilmesi Bilgi Güvenliđi Yöneticisi tarafından yerine getirilir.
- Varlıkların korunması ve politikanın gerçekleştirilmesiyle ilgili güvenlik rollerinin şirket personeline atanması gerçekleştirilir. Hassas sistemlere erişim yetkisi olan yeni ve deneyimsiz kullanıcılar için gerekli gözetimlere dikkat edilir. Çalıřanların sorumluluklarından haberdar olmaları sağlanır.
- Kapsam dahilindeki personel sahip olduđu varlıkların deđerlendirmesini belirlemekten sorumludur.
- Varlıklarda gerçekleşmesi muhtemel ekleme ve çıkarma işlemleri sonrası gerekli durumlarda risk deđerlemesi ve risk raporunun güncellenmesi yapılmalıdır.

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
<b>Bilgi Güvenliđi Yöneticisi</b>	<b>Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim</b>	<b>Yönetim Kurulu</b>

	<b>Bilgi Güvenliği Politikası</b>	
	<b>Doküman No</b>	<b>POL.BS.01</b>
	<b>Doküman Sahibi</b>	<b>Bilgi Sistemleri Yöneticiliği</b>

- Güvenlik sorunları ve bozulmaları BGYS kuruluna raporlanır. Raporlanmış bir güvenlik sorunu öncelikli olarak çözümlenir. Yazılım problemlerinden kaynaklanan sorunlar da aynı şekilde ele alınır.

**Üçüncü Taraf Erişimi:** Üçüncü şahıs ve kurumların bilgi sistemlerine erişimlerinin güvenli olarak gerçekleştirilmesi amacıyla gerekli düzenlemeler yapılır. Bu çerçevede, riskler analiz edilir, erişim gereksinimleri belirlenir ve sınıflandırılır. Anlaşılmalı kurumların personeli ve diğer üçüncü taraflar için ilkeler belirlenir ve uygulanır. Üçüncü taraf erişimleri için uygun risk analizi yapılır. Güvenlik sorumluluklarını da içeren Gizlilik Sözleşmeleri hazırlanır.

**Fiziksel ve Çevresel Güvenlik:** Fiziksel ve çevresel güvenliğin bilgi güvenliği kapsamında eksiksiz olarak sağlanması amacıyla düzenlemeler ve denetimler yapılır. Hassas varlıkların bulunduğu yerler güvenli olmak zorundadır. Güvenli bölgeler bu amaçla hazırlanır ve bu bölgelerin güvenliği sağlanır. İhtiyaca göre farklı güvenlik seviyeleri tanımlanarak her bir seviye için farklı güvenlik mekanizmaları devreye sokulabilir. Donanım güvenliği düşünülerek bu cihazların yetkisiz fiziksel erişim, yangın, su baskını gibi tehdit ve tehlikelere karşı korunması sağlanır. Donanımların yerleştirilmesi, güç kaynaklarının kurulumu, kablolanmanın gerçekleştirilmesi güvenlik düşünülerek yapılır. Donanımların düzenli bakımı gerçekleştirilir. Donanımların yapılandırılması esnasında güvenlik ilkelerine dikkat edilir.

**Denetimler:** Şirket içerisinde Bilgi Güvenliği Yönetim Sistemi kapsamında yılda en az 1 defa iç denetim gerçekleştirilir. Üst Yönetimin gerek görmesi halinde, üçüncü taraf bağımsız denetim uzmanlarından da bağımsız denetim hizmeti veya iç denetimlere danışmanlık hizmeti alınabilir.


**Disiplin Süreci ve Yasal Yükümlülükler:** Tüm çalışanlar, bu politikaya uymakla yükümlüdür. Tüm çalışanlar, çalışma saatleri dışında veya çalışma alanı dışında da bilgi güvenliği ile ilgili yükümlülükler sahiptir. Bilgi Güvenliği Politikası, diğer ilgili politikalar ve BGYS'ni etkileyen süreçlere uyulmaması durumunda ilgili disiplin süreci uygulanır.

## 6. Politikanın Gelişimi

### 6.1. Kalite Kayıtları

<b>Kayıt Ad/Tanımı</b>	<b>Saklandığı Ortam</b>	<b>Sorumlu</b>	<b>Saklama Süresi</b>
<b>Ağ Güvenliği Politikası</b>	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
<b>Erişim Kontrol Politikası</b>	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
<b>Şifre Yönetim Politikası</b>	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
<b>Kabul Edilebilir Kullanım Politikası</b>	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl
<b>İş Sürekliliği Politikası</b>	Ortak Alan	Bilgi Güvenliği Yöneticisi	10 yıl

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
<b>Bilgi Güvenliği Yöneticisi</b>	<b>Bilgi Güvenliği Yönetim Temsilcisi - Üst Yönetim</b>	<b>Yönetim Kurulu</b>

	<b>Bilgi Güvenliđi Politikası</b>	
	<b>Doküman No</b>	<b>POL.BS.01</b>
	<b>Doküman Sahibi</b>	<b>Bilgi Sistemleri Yöneticiliđi</b>

<b>Teçhizat ve Medya Güvenliđi Politikası</b>	Ortak Alan	Bilgi Güvenliđi Yöneticisi	10 yıl
<b>Bilgi Silme Politikası</b>	Ortak Alan	Bilgi Güvenliđi Yöneticisi	10 yıl

### 6.2. Referanslar

- SPK Bilgi Sistemleri Yönetim Tebliđi, ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi Standardı, Madde 5.1 Liderlik ve bađlılık, Madde 5.2 Politika, A.5.1 Bilgi güvenliđi politikaları

### 6.3. Arayüzler

- myHR
- Web Sitesi

<b>Hazırlayan</b>	<b>Kontrol Eden</b>	<b>Onaylayan</b>
<b>Bilgi Güvenliđi Yöneticisi</b>	<b>Bilgi Güvenliđi Yönetim Temsilcisi - Üst Yönetim</b>	<b>Yönetim Kurulu</b>