



Doküman Adı

## Bilgi Güvenliği Politikası

Doküman Kodu

**BG-POL-01**

Yayın Tarihi

**25.02.2021**

Revizyon Numarası

**02**

Revizyon Tarihi

**02.01.2023**

### Hazırlayanlar

İsim Soyisim	Unvan	İmza
Reyyan Aksoy Akkaranfil	Bilgi Güvenliği Yöneticisi	

### Onaylar

İsim Soyisim	Unvan	İmza
Özkan Demir	Genel Müdür	

Bu dokümanın Pisano doküman portalı dışından temin edilen elektronik veya basılı tüm kopyaları KONTROLSÜZ KOPYA olarak değerlendirilmelidir.

### İÇİNDEKİLER

1	AMAÇ.....	3
2	KAPSAM .....	3
3	SORUMLULUK.....	3
3.1	Gözden Geçirme .....	3
4	TANIMLAR VE KISALTMALAR.....	3
5	REFERANSLAR .....	3
6	UYGULAMA.....	3
6.1	Üst Yönetim Taahhüdü .....	3
6.2	Bilgi Güvenliđi Politikası .....	4
6.3	Bilgi Güvenliđi Amaçları .....	4
6.4	Bilgi Güvenliđi Hedefleri .....	5
7	İLGİLİ KAYITLAR.....	5
8	REVİZYON TAKİP ÇİZELGESİ .....	5

## 1 AMAÇ

Bu politikanın amacı, hukuka, yasal, düzenleyici, ya da sözleşmeye tabi yükümlülöklere, iç ve dış tarafların her türlü Bilgi Güvenliđi Yönetim Sistemi gereksinimlerine ilişkin, Üst Yönetim'in bilgi güvenliđi yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri duyurmaktır.

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

Bu politika Bilgi Güvenliđi Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

## 2 KAPSAM

Bu politika, ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi (BGYS) kapsamında bulunan tüm çalışanları ve bilgi varlıklarını kapsamaktadır.

## 3 SORUMLULUK

Pisano Üst Yönetimi, Bilgi Güvenliđi Politikasının tüm çalışanlara ve ilgili üçüncü taraflara duyurulmasını sağlar.

### 3.1 Gözden Geçirme

Bu politika periyodik olarak senede bir defa veya gerekli görülen hallerde Bilgi Güvenliđi Komitesi tarafından gözden geçirilir.

## 4 TANIMLAR VE KISALTMALAR

**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:** Kuruluşun sahip olduđu, işlerini aksatmadan yürütebilmesi için gerekli olan dolayısıyla korumakla yükümlü olduđu varlıklardır.

## 5 REFERANSLAR

ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi Standardı Madde 5.2 : Politika

## 6 UYGULAMA

### 6.1 Üst Yönetim Taahhüdü

Kuruluş Üst Yönetimi bilgi güvenliđinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi, bilgi güvenliđiyle ilgili uygulanabilir yasal şartların ve ISO/IEC 27001 standardı şartlarının yerine getirilmesi için gerekenin yapılacağını taahhüt eder.

Kuruluş bilgi güvenliđi yönetimi ile ilgili olarak aşağıdaki ilkeleri benimsemektedir;

- Müşterilerine ve paydaşlarına sunduđu ürün ve hizmetlere ilişkin faaliyetlerinin güvenliđinin sağlanmasına önem vermektedir.
- Tüm iş süreçlerinin birbiri ile entegre, uyumlu ve dengeli olması hedeflenmektedir. Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliđini ve sürekliliđini gerekli kılmaktadır.
- Müşteri ve paydaşlarına değer sağlayan ürün ve hizmetlerinin gizlilik, bütünlük ve erişilebilirliđini tehdit edebilecek risklere karşı tedbir almayı ilke edinir.

- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliđi hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir.

### 6.2 Bilgi Güvenliđi Politikası

Bilgi güvenliđi, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile mümkündür.

Bilginin;

- Gizlilik gerekliliđi, bilginin sadece yetkili kişiler tarafından erişilebilir olmasını,
- Bütünlük gerekliliđi, bilgi varlıklarının tam ve doğruluğunun sağlanmasını, yetkisiz deđişimlerden korunmasını,
- Erişilebilirlik gerekliliđi, bilgi varlıklarının ihtiyaç duyulduđu anda yetkili kullanıcılar tarafından kullanılabilir olmasını ifade eder.

Pisano bilgi güvenliđini sağlamak amacıyla kendi kurumsal işleyişini düzenleyici prensipler oluşturur. Bilgi Güvenliđi Politikasının belirlenmesi, güvenlik rollerinin tanımlanması ve ilgili tüm güncellemelerin yapılması Üst Yönetim'in desteđi ve tüm birimlerin koordinasyonu ile gerçekleştirilir. Pisano gerekli durumlarda iç ve dış uzmanların görüşüne başvurabilir.

Pisano'da bilgi varlıkları uygun şekilde sınıflandırılır. Varlıkların deđerlemesi yapılır ve uygun seviyede kontrol geliştirmek için varlıkların deđeri hesaplanır.

### 6.3 Bilgi Güvenliđi Amaçları

Kuruluş yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliđi çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi hedefler;

- Bilgi Güvenliđi Yönetim Sistemi (BGYS), uluslararası olarak kabul edilmiş olan ISO/IEC 27001 Bilgi Güvenliđi Yönetim Sistemi standardı şartları doğrultusunda planlanır, gerçekleştirilir ve geliştirilir,
- İlgili kanun ve yönetmeliklere uyumlu hale gelmesi için gereken çalışmalar yapılır,
- BGYS'nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi için gerekli aksiyonlar yönetim ve yönetimin bilgi güvenliđi sorumluluđu verdiği ekipler tarafından sağlanır,
- Bilgi güvenliđi ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır,
- Bilgi güvenliđi yönetim sistemi çerçevesinde gerekli çalışmaların gerçekleştirilmesi için kaynaklar yönetim tarafından sağlanır,
- Paydaşları ile birlikte kuruluşun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir,
- Bilgi Güvenliđi Yönetim Sistemi kapsamı bilgi varlıkları belirlenerek, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliđi beklentileri değerlendirilerek, varsa yasal ve sözleşmeler yükümlülükler analiz edilerek yönetim tarafından iş stratejileri doğrultusunda belirlenir,
- Bilgi varlıklarının sınıflandırılması ve bu varlıkların gizlilik, bütünlük ve erişilebilirlik deđerlendirmesinin yapılabilmesi için varlık envanteri oluşturulur,
- Bilgi güvenliđi risklerini yönetmek için risklerini deđerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilir ve olası riskleri önlemek için çalışmalar gerçekleştirilir,
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliđi hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir,
- Çalışan özlük bilgilerinin mahremiyeti sağlanır,
- Müşteri bilgilerinin yetkisiz kişilerin eline geçmesi engellenir,

- Veri bütünlüğü sağlanır,
- Tedarikçi nezdinde bilgi güvenliđi sağlanır,
- Operasyonel Know-How'ın sürekli geliştirilmesi ve korunması sağlanır,
- Son kullanıcı bilgi güvenliđi farkındalığını ve bu farkındalığın sürekli artırılması sağlanır,
- Bilgi güvenliđini etkin biçimde yöneterek bilgi güvenliđi kaynaklı yaşanabilecek zararlar asgariye indirilir,
- Bilgi güvenliđi ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, yaşanması durumunda koordineli şekilde yanıt verilir,
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediđi durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale gelmesi sağlanır,
- Bilgi Güvenliđi Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliđi, bütünlüğü ve erişilebilirliđi sağlanır. Müşteri ile ilgili kritik iş süreçlerinin devamlılıđı sağlanır,
- Bilgi Güvenliđi Yönetim Sisteminin sürekli iyileştirilmesi sağlanır,
- İnsan kaynakları yönetiminde istihdam öncesi, sırası ve sonrasında güvenliđi sağlama açısından kuralların belirlendiđi süreçler oluşturulur,
- Güvenli çalışma alanları, ofis alanı, depo gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliđin sağlanması için gerekli önlemlerin alınması sağlanır,
- Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi, meydana gelen deđişikliklerin yönetilmesi için prosedür oluşturulur, özellikle bilgi teknolojileri tedarikçileri ile yapılan/yapılacak olan ve bilgi güvenliđi risklerinin ifade edildiđi anlaşmalarda güvenlik gereksinimleri belirlenir.

### 6.4 Bilgi Güvenliđi Hedefleri

BGYS amaçları kapsamında belirlenen ölçülebilir hedefler, Bilgi Güvenliđi Performans Deđerlendirme Formu aracılıđı ile belirlenir, Performans Deđerlendirme ve Sürekli İyileştirme Prosedüründe anlatıldıđı gibi deđerlendirilir ve izlenir.

## 7 İLGİLİ KAYITLAR

- Performans Deđerlendirme ve Sürekli İyileştirme Prosedürü
- Bilgi Güvenliđi Performans Deđerlendirme Formu
- BGYS Kapsam Analizi Dokümanı
- BGYS İlgili Taraf Analizi
- Dokümanların ve Kayıtların Kontrolü Prosedürü
- Yönetim Sistemleri Roller ve Sorumluluklar Dokümanı
- Varlık Yönetim Prosedürü
- Risk ve Fırsat Yönetim Prosedürü
- İç Denetim Prosedürü
- Düzeltici Faaliyet Prosedürü
- İnsan Kaynakları Güvenliđi Prosedürü
- BGYS Fiziksel ve Çevresel Güvenlik Prosedürü
- Üçüncü Taraf Bilgi Güvenliđi Prosedürü
- BT Güvenlik Prosedürü

## 8 REVİZYON TAKİP ÇİZELGESİ

Revizyon No	Revizyon Tarihi	Güncelleme Yapan	Açıklamalar
-------------	-----------------	------------------	-------------

Bu dokümanın Pisano doküman portalı dışından temin edilen elektronik veya basılı tüm kopyaları KONTROLSÜZ KOPYA olarak deđerlendirilmelidir.

01	25.02.2021	Reyyan Aksoy Akkaranfil	İlk yayın
02	02.01.2023	Reyyan Aksoy	Onaycı ismi deđiştirilmiştir