**KORAY GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.**
**BİLGİ GÜVENLİĞİ POLİTİKASI**

## 1. KAPSAM ve YASAL DAYANAK

Bilgi Güvenliği Politikası ***("Politika" veya "BGP")***, Koray Gayrimenkul Yatırım Ortaklığı Anonim Şirketi'nin ***("Koray GYO"*** *veya* ***"Şirket")*** bünyesindeki bilgi varlıklarını kapsamaktadır. Tüm lokasyonlardaki çalışanlar, lokasyon içi ve dışı tedarikçiler / yüklenici tarafından uygulanır.

Bilgi Güvenliği Politikası, halka açık şirketleri için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII-128.9 no.lu Bilgi Sistemleri Yönetimi Tebliği ***("Tebliğ")*** ve Kişisel Verilerin Korunması Kanunu ile diğer düzenlemeler dikkate alınarak hazırlanmıştır.

## 2. AMAÇ

Koray Gayrimenkul Yatırım Ortaklığı A.Ş., kurumsal bilgiyi son derece değerli bir varlık olarak kabul etmektedir. Koray GYO Bilgi Güvenliği Politikası'nın amacı da, Şirket ve bağlı ortaklıklarının iş sürekliliğini sağlamak ve potansiyel tehditlerin etkisini azaltmak için bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlayarak bilgi güvenliği olaylarını engellemek veya hasar riskini minimize etmektir.

Şirket özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini,
- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı,
- Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için gerekli kaynakları sağlamayı, kontrolleri tesis etmeyi, sürekli iyileştirme fırsatlarını değerlendirmeyi ve gözetim için gerekli çalışmaları gerçekleştirmeyi,
- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi,

## 3. BİLGİ GÜVENLİĞİ

Bilgi, diğer önemli ticari ve kurumsal varlıklar gibi, bir şirket için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği iş sürekliliğini sağlamak, kayıpları en aza indirmek için bilgiyi tehlike ve tehdit alanlarından korur. Bilgi güvenliği, Politika'da aşağıdaki bilgi niteliklerinin korunması olarak tanımlanmaktadır:

**Varlık** **:** Şirket için değeri olan her şey (Şirkete ait her türlü bilgi, yazılım, donanım, insan, süreç)

**Bilgi** **:** Çalışma, tecrübe veya öğrenim sonucu elde edilen düşünce ürünü

**Gizlilik** : Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi

**Bütünlük** : Bilginin ve işleme yöntemlerinin doğruluğunun ve yetkisiz değiştirilememesinin temin edilmesi

**Erişilebilirlik**: Yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara en hızlı şekilde erişebileceklerinin garanti edilmesi

**Şirket Bilgisi:** Şirket faaliyetleri sırasında elde edilen, ticari sır olarak nitelendirilebilecek bilgiler ***"Şirket Bilgisi"*** olarak anılacaktır

"Şirket Bilgisi" kapsamına giren bilgiler aşağıda sıralanmıştır:

- Şirket müşterilerine ait her türlü bilgi
- Şirketin üçüncü şahıslarla kurduğu hukuki ilişki(ler) nedeniyle gizlemekle yükümlü olduğu her türlü fikri, mali, ticari, teknik vb. bilgiler
- Pazarlama ve satış planları, ürün geliştirme planları, rekabet analizleri, kıyaslama (benchmark) test sonuçları, iş ve finansal planlar veya öngörüler, ticari sırlar, halka açık olmayan finansal bilgiler, sözleşmeler, Şirket çalışanlarına ait bilgiler,
- Şirket ve sistemlerine ilişkin her türlü bilgi,
- Şirket'in buluşları, gelişmeler, AR-GE çalışmaları, gelişme aşamasındaki çalışmalar, satın alma, muhasebe ve lisanslama ile ilişkili her türlü bilgi, belge veya malzeme,
- Şirket tarafından veya Şirket için dış firmalar tarafından geliştirilmiş veya lisansı alınmış tüm yazılımlar bu kapsamdadır. Burada geçen "yazılım" terimi, yazılım geliştirmenin çeşitli aşamalarını ve bunların sonuçlarını, programın tüm unsurlarını (kaynak kodu, makine kodu vb.), tüm çoğul ortam unsurlarını (menu, ekranlar, yapı, organizasyon, ve benzerlerini), programın her türlü insan veya makine tarafından okunabilen formunu, programın veya bilginin saklandığı, yazıldığı, tanımlandığı, her türlü diyagram, akış tabloları, tasarımlar, çizimler, özellikler, modellemeler, veriler, hata raporları, yordam, belge biçimi ve içerikleri, müşteri veya tedarikçi bilgilerinin bulunduğu basılı veya diğer ortamlar,
- Şirket'in ortak olduğu veya şirket ortaklarının ortak olduğu diğer şirketlere ait yukarıda belirtilmiş bilgiler,
- Yukarıda tanımlanmayan, yasal olarak gizli tutulması gereken veya şirket tarafından gizli olarak nitelendirilen tüm bilgiler.

## 4. YETKİ VE SORUMLULUK

Yönetim Kurulu etkili bir bilgi güvenliği yönetim yapısının tesis edilmesi amacıyla, bilgi güvenliği stratejisi ve yol haritasının belirlendiği Bilgi Güvenliği Politikasını onaylar ve uygulanmasını zorunlu tutar.

Bilgi Güvenliği Politikasının hazırlanması, güncellenmesi ve uygulanmasını Şirket üst yönetimi gözetir, Yönetim Kurulu ise onaylar. Bu konudan sorumlu üst yönetimi ise Şirket Yönetim Kurulu belirler. Bilgi Güvenliği Politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin sağlanması ise Şirket Yönetim Kurulunun sorumluluğundadır.

Bilgi Sistemleri Üst Yönetimi, Finansman & Mali İşler GMY, Hukuk ve Uyum Birimi Yöneticisinden oluşan Şirket'in üst düzey yöneticileri arasından Yönetim Kurulu tarafından atanır.

### 4.1. Bilgi Sistemleri Üst Yönetimi Görev ve Sorumlulukları

i. Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi,
ii. Bilgi Sistemlerinin kullanılmasına ilişkin olarak; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak bilgi güvenliği politikasının hazırlanması,
iii. Bilgi güvenliği politikasının Yönetim Kuruluna sunulması
iv. Bilgi güvenliği politikasının personele duyurulması,
v. Bilgi güvenliği politikasının uygulanması, gözetimi ve kontrolü
vi. Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projelerin gözden geçirilmesi ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanması,
vii. Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis edilmesi,
viii. Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,
ix. Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu

çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,

x. Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
xi. Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi,
xii. Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürlerin, Şirket'in organizasyonel ve yönetsel yapısı içerisinde fiili olarak işleyecek şekilde yerleştirilmesi ve işlerliğine ilişkin gözetim ve takiplerin gerçekleştirilmesi,
xiii. Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanması,
xiv. Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesinin, işletilmesinin, güncelliğinin sağlanması ve gerekli yönetsel sorumlulukların tanımlanması,
xv. Şirket'in sahip olduğu bilgi varlıklarını ve bu varlıkların sorumlularının belirlenmesi, bu varlıkların envanterinin oluşturulması ve envanterin güncelliğinin sağlanması, bilgi varlıklarının önem derecelerine göre sınıflandırılması,
xvi. Fiziksel erişimin yalnızca yetkilendirilmiş kişilerce yapılmasını sağlamak amacıyla, güvenli alanların gerekli giriş kontrolleriyle korunmasının sağlanması,
xvii. Yangın, sel, deprem, patlama, yağma ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanması ve uygulanması,
xviii. Ağların tehditlere karşı korunması ve ağları kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kontroller tesis edilmesi ve etkin bir şekilde yönetilmesi,
xix. Bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemlerin alınması,
xx. Bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemlerin alınması,
xxi. Bilgi sistemleri üzerindeki risklerin, sistem veya faaliyetlerin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizmasının tesis edilmesi,
xxii. Yönetim Kurulu'nun onayı ile bu hizmetlerin dışarıdan alınmasına ilişkin iş ve işlemlerin yürütülmesi.

**4.2. Çalışan ve Üçüncü Kişi Sorumluluğu**

Bilgi Güvenliği Politikası'na uyum ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, Koray GYO ve/veya bağlı ortaklık bilgilerini veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve Koray GYO bilgilerine, sağladığı hizmet nedeniyle erişimi olan üçüncü kişi hizmet sağlayıcıları ve bunların bağlı destek personelinin Politika düzenleme ve yükümlülüklerine bağlı hareket etmesi şarttır.

Şirket bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişenler:

i. Kişisel ve elektronik iletişimde Şirket'e ait bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlarlar.
ii. Risk düzeylerine göre belirlenen güvenlik önlemlerini alırlar
iii. Bilgi güvenliği ihlal olaylarını Bilgi Sistemleri Üst Yönetimi'ne bildirerek raporlar ve bu ihlalleri engelleyecek önlemleri alırlar.
iv. Şirket içi bilgi kaynaklarını (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletmezler.
v. Şirket bilişim kaynaklarını, mevzuata aykırı faaliyetler amacıyla kullanmazlar.
vi. Yatırımcılar, iş ortakları, tedarikçiler veya diğer üçüncü kişilere ait bilgilerin gizliliğini,

bütünlüğünü ve erişilebilirliğini korurlar.

Şirket Yönetimi (veya Bilgi Sistemleri Üst Yönetimi), Bilgi Güvenliği Politikası doğrultusunda, tüm çalışanlarının bilgi güvenliği konularıyla ilgili farkındalık eğitimleri almalarını temin eder ve Politika'ya uyumunu sağlar.

## 5. KONTROL ve GÖZETİM

Bilgi Güvenliği Politikası ihlalleri, Şirket'in risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca hukuki, idari ve/veya cezai sorumluluğuna sebep olabilecektir. Dolayısıyla, Politika'da açıkça düzenlenen kontrol ve gözetim sorumlulukları dışında, Şirket'in her birim yöneticisi de Bilgi Güvenliği Politikası'na uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetmekten birinci derece sorumludur.

Şirketin saygınlık ve güvenirliğini korumak için şüphe uyandırıcı herhangi bir durumu bildirmek tüm çalışanlarımızın bireysel sorumluluğudur.

Bilgi Güvenliği Politikası ve Alt politikalarda belirtilen hususlara, bilgi güvenliği standartlarına ve yönergelerine uyulmaması nedeniyle Şirketin itibar veya maddi zararına neden olunmuşsa, bu konuda Şirket Disiplin hükümleri uygulanır.

Fark edildiği halde bilgi güvenliği ihlal ve zayıflıklarının bildirilmemesi, görmezden gelinmesi, BGP' nin ihlal edilmesi kapsamında değerlendirilecek olup, disiplin soruşturmasına konu olabilecektir.

## 6. YÜRÜRLÜLÜK

İşbu Bilgi Güvenliği Politikası, Yönetim Kurulu'nun veya Yönetim Kurulu tarafından yetkilendirilen Yönetim Kurulu Üyelerinin imza tarihinde yürürlüğe girer.