Yürürlülük Tarihi:	01.10.2025
Revizyon No:	00

İSTİNYEPARK İSTANBUL GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş
BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç ve Yaklaşım

1.1 Bu politikanın amacı, İstinyePark İstanbul Gayrimenkul Yatırım Ortaklığı A.Ş. (İstinyePark İstanbul GYO)'nun sahip olduğu tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmasını sağlamak; bilgi güvenliği risklerini yönetmek, yasal gerekliliklere uyumu garanti altına almak ve bilgi güvenliği kültürünü kurumsal düzeyde yerleştirmek ve bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların belirlenmesini ve görev tanımlarının yapılmasını, hedeflerin belirlenmesini, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini, değerlendirilmesini ve gözetimini sağlamaktır.

1.2 Politika, Sermaye Piyasası Kurulu (SPK) Bilgi Sistemleri Yönetimi Tebliği, Kişisel Verilerin Korunması Kanunu (KVKK), Türk Ticaret Kanunu (TTK) ve ISO/IEC 27001:2022 standardı esas alınarak hazırlanmıştır.

2. Kapsam

2.1 Bu politika, şirketin tüm çalışanlarını, yönetim kurulu üyelerini, danışmanlarını, iş ortaklarını, tedarikçilerini ve üçüncü taraf hizmet sağlayıcılarını kapsar.

2.2 Politika, şirketin sahip olduğu veya işlettiği tüm bilgi sistemlerini, verileri, altyapıyı, uygulamaları ve elektronik iletişim araçlarını içerir.Bilgi güvenliği, tüm çalışanların ve paydaşların ortak sorumluluğudur.

3. Yönetişim Yapısı

3.1 Yönetim Kurulu, bu politikanın onaylanmasından, sorumludur. Bilgi güvenliği yönetim sistemi kapsamındaki risklerin ve kontrollerin şirket stratejileriyle uyumlu olmasını sağlar. Bilgi Güvenliği yönetimiyle ilgili konularda Yönetim Kurulu tarafından Genel Müdür Üst Yönetim olarak seçilmiştir. Üst Yönetim Politikanın uygulanması için gerekli kaynakların (insan, finansal, teknolojik) tahsis edilmesini güvence altına alır. Bilgi Güvenliği Komitesi'nin raporlarını periyodik olarak inceler, gerekli düzeltici ve önleyici aksiyonların alınmasını sağlar. Üst Yönetim , bilgi güvenliği ve siber riskler konusunda farkındalık düzeyini korumakla yükümlüdür..

3.2 Üst Yönetim Politikanın uygulanması için gerekli organizasyonel ve teknik kaynakları tahsis eder.

3.3 Bilgi Güvenliği Komitesi (BGK) Bilgi güvenliği stratejilerini belirler, riskleri değerlendirir, siber olay ve denetim sonuçlarını inceler. BGK, bilgi güvenliğine ilişkin çalışmaların koordinasyonunu sağlamak, sistemin işlerliğini takip etmek ve iyileştirme önerilerini

değerlendirerek karara bağlamak, bilgi güvenliği projeleri ve sertifikasyon süreçlerini takip etmek ve hakkında Yönetime bilgi vermek, sorumlu olduğu alanlara yönelik politika, prosedür, yönetmelik vb. dokümanların güncelleme gereksinimlerini takip etmek, güncelliğini sağlamak üzere aksiyon almak, bilgi güvenliği farkındalığı çalışmaları ve eğitim programlarını değerlendirmek ve Üst Yönetim'e raporlama yapmakla sorumludur. BGK, üç ayda bir toplanır,Üst Yönetim'e rapor verir.

3.4 Bilgi Güvenliği Sorumlusu (IT Müdürü) Güvenlik kontrollerinin uygulanmasından, Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden, takibinden, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi, üst yönetime rapor verilmesinden, bilgi sistemleri iç kontrolünden, bilgi sistemleri denetiminden, bilgi sistemleri yönetiminden, olay yönetiminden ve farkındalık eğitimlerinden sorumludur.

3.5 Çalışanlar Bilgi güvenliği politikalarına uymak ve güvenlik ihlallerini derhal raporlamakla yükümlüdür.

4. Yasal ve Düzenleyici Uyum

4.1 Sermaye Piyasası Kurulu (SPK) Mevzuatı: Şirket, SPK Bilgi Sistemleri Yönetimi Tebliği'nde belirtilen tüm yükümlülüklere uyar. Bilgi sistemleri sızma testleri (penetration tests) yılda en az bir kez, Tebliğ'deki Bilgi Sistemleri Sızma Testleri Usul ve Esasları'na uygun şekilde gerçekleştirilir. Tespit edilen zafiyetler giderilir, doğrulama testleri yapılır ve sonuçlar Bilgi Güvenliği Komitesi'ne raporlanır.

4.2 Kişisel Verilerin Korunması Kanunu (KVKK): Kişisel veriler KVKK hükümlerine uygun olarak işlenir, aktarılır ve korunur; ihlaller 72 saat içinde Kurum'a bildirilir.

4.3 Diğer Mevzuatlar: Elektronik kayıtlar TTK hükümlerine uygun olarak korunur ve sözleşmelerde bilgi güvenliği hükümleri yer alır.

5. Bilgi Güvenliği İlkeleri

5.1 Gizlilik (Confidentiality): Bilgiye yalnızca yetkili kişiler erişebilir.

5.2 Bütünlük (Integrity): Bilgilerin doğruluğu ve bütünlüğü korunur.

5.3 Erişilebilirlik (Availability): Bilgi varlıklarına ihtiyaç duyulduğunda erişim sağlanır.

5.4 İzlenebilirlik (Traceability): Tüm erişim ve işlemler kayıt altına alınır.

5.5 Uyumluluk (Compliance): Faaliyetler yasal ve düzenleyici gerekliliklere uygun yürütülür.

5.6 Veri Sahipliği ve Sorumlulukları (Data Ownership)

5.6.1 Her bilgi varlığı için bir Veri Sahibi (Data Owner) ve Veri Sorumlusu (Data Custodian) atanır.

5.6.2 Veri Sahibi, verinin sınıflandırılması, doğruluğu ve erişim onaylarından sorumludur.

5.6.3 Veri Sorumlusu, verinin korunması, yedeklenmesi ve erişim kontrolünün uygulanmasından sorumludur.

5.6.4 Tüm bilgi varlıkları Bilgi Varlığı Envanteri üzerinde kayıt altına alınır ve yılda en az bir kez gözden geçirilir.

6. Teknik Güvenlik Kontrolleri

6.1 Ağ Güvenliği: Ağ altyapısı, endüstri standardı güvenlik çözümleriyle korunur.

6.2 Kimlik ve Erişim Yönetimi: Kullanıcı kimlikleri merkezi olarak yönetilir; görev bazlı yetkilendirme yapılır.

6.3 Veri Koruma: Hassas veriler endüstri standardı kriptografik algoritmalarla korunur; veri aktarımı güvenli yöntemlerle yürütülür.

6.4 İzleme ve Log Yönetimi: Bilgi sistemleri faaliyetleri gelişmiş analitik sistemlerle izlenir; loglar bütünlüğü korunarak saklanır.

6.5 Yedekleme ve Felaket Kurtarma: Kritik sistemler için BIA (Business Impact Analysis – İş Etki Analizi) yapılır; RTO (Recovery Time Objective – Kurtarma Süresi Hedefi) ve RPO (Recovery Point Objective – Kurtarma Noktası Hedefi) hedefleri tanımlanır.

7. İdari Güvenlik Önlemleri

7.1 İşlenen tüm kişisel verilerin neler olduğu belirlenir, bu verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığı ve gerçekleşmesi durumunda yol açacağı kayıpların doğru bir şekilde belirlenerek buna uygun tedbirlerin alınır.

7.2 Bu risklerin tanımlanması ve önceliğinin belirlenmesinden sonra; söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilir, gerekli teknik ve idari tedbirler planlanarak uygulamaya konulur.

7.3 Kişisel veri güvenliğine ilişkin belirlenecek politika ve prosedürler, çalışma ve işleyişe uygun şekilde entegre edilir. Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılır, yapılan kontroller belgelenir, geliştirilmesi gereken hususlar belirlenir ve gerekli güncellemeler yerine getirildikten sonra da düzenli olarak kontrollere devam edilir.

7.4 Çalışanlar gizlilik taahhütnamesi imzalar ve işten ayrılan personelin erişimi aynı gün sonlandırılır.

7.5 Fiziksel erişim kontrolleri yalnızca yetkili personele tanımlanır.

7.6 Yetkilendirmeler minimum yetki ilkesine esas alınarak tanımlanır ve erişimler düzenli aralıklarla gözden geçirilir.

7.7 Çalışanların güvenlik politika ve prosedürlerine uymaması durumunda devreye girecek bir disiplin prosedürü yürütülür.Kişisel veri güvenliğine ilişkin çalışanlara eğitim verilir. Eğitim programı yılda en az bir kez tekrarlanır ve güncel tehdit ortamına göre güncellenir. Düzenli aralıklarla oltalama (phishing) simülasyonları yapılır; bu testlerin sonuçlarına göre personele hedeflenmiş ek eğitimler atanır. Eğitim performansları ölçülür ve Bilgi Güvenliği Komitesi'ne raporlanır.

7.8 Şirket içi periyodik ve/veya rastgele denetimler gerçekleştirilir.

7.8 Veri işleyenler ve veri sorumluları ile yapılacak sözleşmelerde veri işleyenin sadece veri sorumlusunun talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaç ve kapsamına uygun ve kişisel verilerin korunması mevzuatı ile uyumlu şekilde hareket edeceği, Kişisel Veri Saklama ve İmha Politikasına uygun hareket edeceğii, işlediği kişisel verilere ilişkin olarak süresiz sır saklama yükümlülüğüne tabi olacağı, herhangi bir veri ihlali olması durumunda, veri işleyenin bu durumu derhal veri sorumlusuna bildirmekle yükümlü olacağı belirtilir.

7.9 Sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel veriler, daha güvenli ortamlarda muhafaza edilir ve İhtiyaç duyulmayan kişisel verilerin kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve güvenli bir şekilde imha edilmesi sağlanır.

7.10 Herhani bir veri ihlali halinde kriz yönetimi yapılır ve Kuruma ve ilgili kişi bildirimleri gerçekleştirilir.

Olay Yönetimi ve Müdahale

8.1 Siber Olay Müdahale Ekibi (CSIRT – Computer Security Incident Response Team) olay yönetiminden sorumludur; olaylar kritik, yüksek, orta ve düşük olarak sınıflandırılır.

8.2 Olay kayıtları tutulur, kök neden analizi yapılır ve önleyici faaliyetler uygulanır.

8.3 İstibyePark GYO Veri İhlali Müdahale Planı kapsamında prosedüler izlenir ve gerekli tüm idari ve teknik tedbirler alınır. KVKK ihlalleri 72 saat içinde Kuruma bildirilir; SPK kapsamındaki olaylar ilgili otoritelere raporlanır.Ayrıca veri ihlalinden etkilenen ilgili kişilere makul süre içerisinde bildirim yapılır.

8.4 Performans KPI (Key Performance Indicator – Anahtar Performans Göstergesi) ve KRI (Key Risk Indicator – Anahtar Risk Göstergesi) metrikleriyle izlenir.

9 Üçüncü Taraf ve Tedarikçi Yönetimi

9.1 Tedarikçiler ve üçüncü taraflar bilgi güvenliği risk değerlendirmesine tabi tutulur ve yıllık denetim yapılır. Bulut hizmet sağlayıcılarının ISO 27001 sertifikasına sahip olması beklenir. Bilgi içeren ortamları, üçüncü taraflar ile yapılan veri aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korunur. Bu kapsamda yapılan çalışmalar yazılı hale getirilir ve veri aktarımlarına ilişkin denetim izi tutulur.

10 İş Sürekliliği, Yedekleme ve Veri İmhası

10.1 Şirket, kritik iş süreçlerinin kesintisiz devamını sağlamak amacıyla İş Sürekliliği Planı (Business Continuity Plan – BCP) oluşturur. Bu plan, felaket, siber saldırı, altyapı arızası veya insan kaynaklı olaylarda devreye girer.

10.2 Kritik süreçler için BIA (Business Impact Analysis – İş Etki Analizi) yapılır ve RTO (Recovery Time Objective – Kurtarma Süresi Hedefi) ile RPO (Recovery Point Objective – Kurtarma Noktası Hedefi) değerleri belirlenir.

10.3 İş Sürekliliği Planı yılda en az bir kez test edilir ve test sonuçları Bilgi Güvenliği Komitesi tarafından değerlendirilir.

10.4 Tüm sistem ve veri yedeklemeleri, 3-2-1 kuralına göre yürütülür: 3 kopya: Verilerin en az üç kopyası bulundurulur (birincil, ikincil, yedek). 2 ortam: Yedekler iki farklı ortamda (örneğin disk ve bulut, ya da disk ve manyetik bant) saklanır. 1 dış konum: En az bir kopya farklı fiziksel konumda (off-site) veya güvenli bulut altyapısında tutulur. Yedekler düzenli olarak doğrulanır; bütünlük kontrolleri (checksum/validation) uygulanır. Kritik sistem yedeklemeleri günlük, standart sistem yedeklemeleri haftalık olarak gerçekleştirilir. Yedekleme süreçleri otomatik sistemlerle izlenir ve başarısız işlemler Bilgi Güvenliği Sorumlusuna raporlanır. Yedek veriler, erişim yetkileri sınırlı personel tarafından yönetilir ve endüstri standardı kriptografik yöntemlerle şifrelenir. Yedekleme kayıtları ve logları en az 1 yıl süreyle saklanır.

10.5 Veriler, ilgili yasal düzenlemelerde öngörülen saklama süreleri boyunca muhafaza edilir. Saklama süresi dolan veriler, geri döndürülemeyecek şekilde silinir veya fiziksel imha edilir. Kişisel veriler, KVKK'ya uygun biçimde anonimleştirilerek veya takma adlandırma yöntemiyle korunabilir. İmha faaliyetleri kayıt altına alınır ve bu kayıtlar en az 3 yıl süreyle saklanır.Veri imha işlemleri, "Veri Saklama ve İmha Politikası"na uygun şekilde yürütülür.

11 Politika Hiyerarşisi

11.1 Politika, Bilgi Güvenliği Prosedürü, Erişim Kontrol Prosedürü, Veri Saklama Politikası vb. belgelerle birlikte yürütülür.

12 Yürürlük

12.1 Bu politika 01.09.2025 tarihinde Yönetim Kurulu onayıyla yürürlüğe girmiştir; yılda en az bir kez gözden geçirilir.