1. Amaç

Bu Bilgi Güvenliği Politikasının amacı; Kızılbük Gayrimenkul Yatırım Ortaklığı A.Ş.'nin, Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) hükümlerine uyum sağlaması ile Şirketin bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını ve bilgi sistemlerinin güvenli, sürdürülebilir ve mevzuata uygun şekilde yönetilmesini sağlamaktır.

Bu politika, Tebliğ kapsamında öngörülen bilgi güvenliği yönetişim çerçevesini ortaya koyar. Detaylı uygulama, kontrol ve operasyonel süreçler; bu politika altında yürürlüğe konulan prosedür ve talimatlar aracılığıyla yürütülür.

2. Kapsam

Bu politika;

- Şirketin sahip olduğu veya sorumluluğunda bulunan tüm bilgi varlıklarını,
- Bilgi sistemlerini (donanım, yazılım, ağ altyapısı ve uygulamalar),
- Şirket çalışanlarını, yöneticilerini ve bilgi sistemlerine erişimi bulunan üçüncü tarafları

kapsar.

3. Dayanak ve Mevzuat

Bu Bilgi Güvenliği Politikası;

Sermaye Piyasası Kurulu'nun Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10) başta olmak üzere, Şirketin tabi olduğu ilgili mevzuat ve düzenlemeler esas alınarak hazırlanmıştır.

Politika, Tebliğ kapsamında bilgi güvenliğine ilişkin öngörülen yükümlülüklerin kurumsal düzeyde yerine getirilmesini sağlamak amacıyla oluşturulmuştur.

4. Temel İlkeler

Şirket, bilgi güvenliğini aşağıdaki temel ilkeler doğrultusunda ele alır:

- Gizlilik: Bilgiye yalnızca yetkili kişiler erişebilir.
- Bütünlük: Bilgi, yetkisiz veya hatalı şekilde değiştirilemez.
- Erişilebilirlik: Yetkili kullanıcılar, ihtiyaç duyduklarında bilgiye erişebilir.

Bilgi güvenliği; Şirketin risk yönetimi, iç kontrol ve kurumsal yönetişim yapısının ayrılmaz bir parçasıdır.

5. Yönetim ve Sorumluluklar

- Yönetim Kurulu, bilgi güvenliğine ilişkin nihai gözetim ve onay merciidir.
- Üst yönetim, bu politikanın uygulanmasını sağlar ve izler.
- Çalışanlar ve üçüncü taraflar, bilgi güvenliği ile ilgili politika, prosedür ve talimatlara uymakla yükümlüdür.

6. Bilgi Güvenliği Risk Yönetimi

Bilgi sistemlerine ilişkin riskler; belirlenir, analiz edilir, değerlendirilir ve uygun kontrol mekanizmaları ile yönetilir.

Risk yönetimi faaliyetleri, bu politika kapsamında yürürlüğe konulan Bilgi Güvenliği Risk Yönetimi Prosedürü çerçevesinde yürütülür.

7. Bilgi Güvenliği İhlalleri ve Olay Yönetimi

Bilgi güvenliği ihlalleri ve siber olaylara müdahale; olayın etkilerinin en aza indirilmesi, mevzuata uygun bildirimlerin yapılması ve tekrarının önlenmesi esaslarına dayanır.

Bu kapsamda izlenecek süreçler SOME Müdahale Planı ve Prosedürü ile düzenlenir.

8. Bilgi Varlıkları Yönetimi

Bilgi varlıklarının sınıflandırılması, etiketlenmesi, korunması, kullanımı ve kullanım ömrü sonunda güvenli şekilde silinmesi veya imha edilmesi; ilgili prosedür ve talimatlar çerçevesinde yürütülür.

9. Politikanın İzlenmesi ve Güncellenmesi

Bu politika; mevzuat değişiklikleri, organizasyonel ihtiyaçlar ve risk değerlendirme sonuçları dikkate alınarak en az yılda bir kez gözden geçirilir ve gerekli görülmesi halinde güncellenir.

10. Yürürlük

Bu Bilgi Güvenliği Politikası, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer.

11. Referans Belgeler

Bu politika kapsamında yürürlükte olan uygulama belgeleri aşağıda yer almaktadır:

Belge Adı

- Bilgi Güvenliği Risk Yönetimi Prosedürü
- SOME Müdahale Planı ve Prosedürü
- Bilgi Varlıkları Sınıflandırması ve Etiketleme Talimatı
- Kullanımdan Kalkan Cihazlar için Güvenli Silme ve İmha Prosedürü
- Görevler Ayrılığı Prosedürü