DAĞ GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bu politikanın temel amacı, halka açık bir kurum olarak yatırımcıların hak ve yararlarının korunmasını sağlamak; bilgi varlıklarına zamanında, eksiksiz ve kesintisiz erişimi güvence altına alarak güven ve açıklık ilkeleriyle çalışmaktır. Şirketimiz, bilgi güvenliğini faaliyetlerinin temel ilkelerinden biri olarak kabul eder ve tüm paydaşlarına ait bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmasını, risklerin sistematik olarak yönetilmesini hedefler.

2. Kapsam

Bu politika; şirketin tüm çalışanlarını, yönetim kurulu üyelerini, danışmanlarını, iş ortaklarını ve üçüncü taraf hizmet sağlayıcılarını kapsar. Şirketin sahip olduğu tüm bilişim sistemleri, veriler, altyapı ve elektronik iletişim araçları bu politikanın içeriğine dâhildir.

3. Yasal ve Düzenleyici Uyum

Şirketimiz, faaliyetlerini aşağıdaki yasal mevzuat ve standartlar çerçevesinde yürütmeyi taahhüt eder:

- **Sermaye Piyasası Kurulu (SPK):** Bilgi Sistemleri Yönetimi Tebliği'ne tam uyum sağlanır ve yılda en az bir kez sızma testleri gerçekleştirilir
- **KVKK:** Kişisel veriler kanuna uygun işlenir; olası ihlaller 72 saat içinde ilgili kurumlara bildirilir
- **ISO/IEC 27001**: Bilgi Güvenliği Yönetim Sistemi (BGYS) bu standart esas alınarak yapılandırılır ve sürekli iyileştirilir
- **Türk Ticaret Kanunu (TTK):** Elektronik kayıtlar mevzuata uygun şekilde muhafaza edilir.

4. Yönetişim ve Sorumluluklar

- **Yönetim Kurulu:** Politikanın onaylanmasından ve stratejilerle uyumundan sorumludur.
- **Üst Yönetim:** Sistemin işletilmesi için gerekli insan, finans ve teknoloji kaynağını tahsis eder.
- **Bilgi Güvenliği Sorumlusu:** Güvenlik kontrollerinin uygulanması, olay yönetimi ve farkındalık eğitimlerinden sorumludur.
- **Çalışanlar:** Politikalara uymak ve şüphe duyulan güvenlik açıklarını derhal raporlamakla yükümlüdür.

5. Bilgi Güvenliği İlkeleri ve Kontroller

- **Gizlilik, Bütünlük, Erişilebilirlik:** Bilgiye sadece yetkililer erişebilir, doğruluğu korunur ve ihtiyaç duyulduğunda hazırdır .
- **Varlık Yönetimi:** Her bilgi varlığı için bir "Veri Sahibi" ve "Veri Sorumlusu" atanır; varlık envanteri yılda en az bir kez gözden geçirilir
- **Erişim Yönetimi:** "Minimum yetki" ilkesi esastır; işten ayrılan personelin yetkileri aynı gün sonlandırılır.
- **Teknik Güvenlik**: Hassas veriler kriptografik yöntemlerle korunur, tüm sistem faaliyetleri loglanır ve izlenir.

6. İş Sürekliliği ve Yedekleme

Kritik iş süreçlerinin kesintisiz devamı için İş Sürekliliği Planı (BCP) oluşturulur ve yılda en az bir kez test edilir. Veri yedeklemelerinde 3-2-1 kuralı uygulanır:

- Verinin en az 3 kopyası bulundurulur.
- Yedekler 2 farklı ortamda (disk, bulut vb.) saklanır.
- En az 1 kopya farklı bir fiziksel konumda (off-site) tutulur.

7. Olay Yönetimi ve Müdahale

Olaylar önem derecesine göre sınıflandırılır, kök neden analizi yapılır ve yatırımcı güvenini sarsmayacak şekilde şeffaflıkla yönetilir.

8. Üçüncü Taraf Yönetimi

Hizmet alınan tedarikçiler bilgi güvenliği risk değerlendirmesine tabi tutulur. Bulut hizmet sağlayıcılarının ISO 27001 sertifikasına sahip olması beklenir ve veri aktarımları sözleşmelerle güvence altına alınır.

9. Taahhüdümüz

Kurumsal itibarımızı ve paydaşlarımızın güvenini korumak adına, Bilgi Güvenliği Yönetim Sistemi'ni kurum kültürümüzün ayrılmaz bir parçası olarak uygulamayı ve sürekli iyileştirmeyi beyan ederiz.