# GRAINTURK HOLDİNG ANONİM ŞİRKETİ
# BİLGİ GÜVENLİĞİ POLİTİKASI

## 1. Amaç

Bu politika, GRAINTURK HOLDİNG ANONİM ŞİRKETİ ("**Şirket**")'nin, Sermaye Piyasası Kurulu'nun ("**SPK**") VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği başta olmak üzere ilgili tüm mevzuatlara uygun şekilde bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin olarak, bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanması amacıyla hazırlanmıştır.

Bu politika, 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 temin eder.

## 2. Kapsam

Bu politika;

- Şirket'in tüm ofis ve tesislerinde kullanılan tüm bilgi sistemlerini,
- Donanım, yazılım, veri tabanları, ağ altyapıları ve iletişim sistemlerini,
- Finansal raporlama, kamuyu aydınlatma ve yatırımcı ilişkileri süreçlerini destekleyen sistemleri,
- Kritik ve kritik olmayan uygulamaları,
- Şirket çalışanlarını, yöneticilerini ve yetkilendirilmiş kullanıcıları,
- Bilgi sistemleri kapsamında hizmet alınan üçüncü tarafları ve dış hizmet sağlayıcıları

kapsar.

## 3. Dayanak

Bu politika, SPK VII-128.10 Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği, SPK II-17.1 Kurumsal Yönetim Tebliği, Türk Ticaret Kanunu, Sermaye Piyasası Kanunu, ilgili ikincil düzenlemeler ve rehberler esas alınarak hazırlanmıştır.

## 4. Tanımlar ve Kısaltmalar

- **Bilgi Sistemleri (BS):** Donanım, yazılım, veri, ağ ve insan kaynağından oluşan bütün.
- **Kritik Bilgi Sistemleri:** Kesintisi veya güvenlik ihlali halinde Şirket'in finansal durumu, kamuyu aydınlatma yükümlülükleri veya faaliyet sürekliliğini önemli ölçüde etkileyen sistemler.
- **RTO/RPO:** Kurtarma süresi ve veri kaybı hedefleri.

## 5. Yönetim ve Yönetişim İlkeleri

- Bilgi sistemleri yönetimi, kurumsal yönetimin ayrılmaz bir parçasıdır.

- Yönetim Kurulu, bilgi sistemlerine ilişkin risklerin gözetiminden nihai olarak sorumludur.
- Bilgi sistemleri, risk temelli ve dokümante edilmiş süreçler çerçevesinde yönetilir.
- Görevlerin ayrılığı, hesap verebilirlik ve izlenebilirlik esas alınır.

## 6. Organizasyonel Yapı ve Sorumluluklar

### 6.1 Yönetim Kurulu

Yönetim Kurulu;

- Bilgi sistemleri yönetimine ilişkin politika ve stratejileri onaylar,
- Bilgi sistemleri kaynaklı riskleri ve siber tehditleri gözetir,
- Kritik sistemlere ilişkin iş sürekliliği ve olağanüstü durum kurtarma süreçlerini izler,
- Gerekli organizasyonel yapı, kaynak ve yatırımların tesis edilmesini sağlar,
- Bilgi sistemleri riskleri, iş sürekliliği test sonuçları ve önemli bilgi güvenliği olaylarına ilişkin raporları yılda en az bir kez değerlendirir,
- Gerekli gördüğü hâllerde bilgi sistemleri risklerine ilişkin özel rapor talep edebilir.

### 6.2 Üst Yönetim

Üst Yönetim;

- Politika'nın uygulanmasını sağlar,
- Bilgi sistemleri performansı ve risklerine ilişkin raporları düzenli olarak Yönetim Kurulu'na sunar,
- Risk yönetimi fonksiyonları ile koordinasyonu temin eder.

### 6.3 Bilgi Güvenliği Sorumlusu

Bilgi Güvenliği Sorumlusu;

- Bilgi sistemlerinin güvenli, kesintisiz ve mevzuata uyumlu şekilde işletilmesinden sorumludur,
- Sistem kontrollerini tesis eder, dokümante eder ve etkinliğini izler,
- Bilgi sistemleri riskleri ve güvenlik önlemlerinin etkinliği hakkında üst yönetime raporlama yapar,
- En az 5 yıl bilgi sistemleri güvenliği, yönetişimi, iç kontrol veya denetim alanlarında tecrübeye sahiptir,
- Günlük operasyonel işleyişe dâhil değildir ve doğrudan üst yönetime bağlı çalışır.

### 6.4 Risk Yönetimi

- Bilgi sistemlerine ilişkin risk ve kontrolleri değerlendirir.
- Bulguları üst yönetime ve gerekli hallerde Yönetim Kurulu'na raporlar.

## 7. Bilgi Güvenliği Yönetimi

- Bilgi varlıkları gizlilik, bütünlük ve erişilebilirlik kriterlerine göre sınıflandırılır.
- Erişim yetkileri asgari yetki ve görevlerin ayrılığı ilkelerine göre tanımlanır.

- Kimlik doğrulama, yetkilendirme, loglama, izleme kontrolleri uygulanır ve olay yönetimi mekanizmaları tesis edilir.
- Siber güvenlik tehditlerine karşı önleyici ve tespit edici kontroller uygulanır.
- Bilgi güvenliği olayları kayıt altına alınır, analiz edilir ve raporlanır.

**8. Bilgi Sistemleri Risk Yönetimi**

- Bilgi sistemlerine ilişkin riskler yılda en az bir kez değerlendirilir.
- Kritik riskler için aksiyon planları oluşturulur.
- Risklerin tamamen ortadan kaldırılamayacağı ve her durumda artık risk bulunacağı kabul edilir; artık riski en aza indirecek düzeltici ve önleyici kontroller uygulanır.
- Kabul edilen riskler üst yönetim ve ilgili komitelerin onayına tabidir.

**9. Değişiklik ve Geliştirme Yönetimi**

- Bilgi sistemlerinde yapılan tüm değişiklikler kayıt altına alınır.
- Değişiklikler test, onay ve geri dönüş planları ile yönetilir.
- Canlı ortama geçişler yetkilendirilmiş kişiler tarafından gerçekleştirilir.

**10. İş Sürekliliği ve Olağanüstü Durum Kurtarma Yönetimi**

- Kritik Bilgi Sistemleri için iş sürekliliği ve olağanüstü durum kurtarma planları hazırlanır.
- RTO ve RPO hedefleri tanımlanır ve Yönetim Kurulu gözetiminde izlenir.
- Planlar düzenli olarak test edilir ve sonuçları raporlanır.

**11. Üçüncü Taraf ve Dış Hizmet Yönetimi**

- Dış hizmet alımlarında bilgi güvenliği ve gizlilik hükümleri sözleşmelere dahil edilir.
- Hizmet sağlayıcıların performansı ve riskleri izlenir.
- Dışarıdan alınan yazılım, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını barındıran cihaz/sistemlerin, mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıklarını barındırmadığına yönelik taahhütname; dağıtıcı, tedarikçi veya üreticiden alınır.

**12. İzleme, Raporlama ve Denetim**

- Bilgi sistemleri performansı ve güvenliği düzenli olarak izlenir.
- İç ve dış denetim sonuçları üst yönetime raporlanır.
- SPK ve ilgili otoritelere yapılması gereken bildirimler zamanında gerçekleştirilir.

**13. Eğitim ve Farkındalık**

- Çalışanlara düzenli bilgi güvenliği ve farkındalık eğitimleri verilir.
- Yazılım geliştirme süreçlerinde görevli personelin güvenli yazılım geliştirme konusunda eğitim alması sağlanır.
- Yazılım geliştirme süreçlerinde görevli personelin güvenli yazılım geliştirme konusunda eğitilmesi sağlanır.

## 14. Yürürlük ve Gözden Geçirme

İşbu Bilgi Güvenliği Politikası 30/12/2025 itibarıyla Yönetim Kurulu onayı ile yürürlüğe girmiştir.

Politika; en az yılda bir kez veya mevzuat ve organizasyonel değişiklikler doğrultusunda gözden geçirilir, iş ihtiyaçları ile değişen tehdit ve risklere göre güncellenir.

**Onaylayan:** Yönetim Kurulu
**Yürürlük Tarihi:** 30/12/2025