KUVEYTTÜRK
Yatırım

BİLGİ GÜVENLİĞİ POLİTİKASI

RİSK YÖNETİMİ

İÇİNDEKİLER

1. AMAÇ 2
2. KAPSAM 2
3. SORUMLULUK 2
   3.1 Yönetim Kurulu 2
   3.2 Bilgi Güvenliği Sorumlusu 2
   3.3 Şirket Çalışanı 3
4. KISALTMALAR VE TANIMLAR ..... Error! Bookmark not defined.
5. UYGULAMA 4
6. İSTİSNA 5
7. İLGİLİ DOKÜMANLAR 5
8. YÜRÜRLÜLÜK 5
9. REVİZYON TAKİP ÇİZELGESİ 5

HAZIRLAYAN / REVİZE EDEN	*KONTROL EDEN*	*ONAYLAYAN*
Kıdemli Bilgi Güvenliği Uzmanı	Üst Yönetim	Yönetim Kurulu

1. AMAÇ

Bu politikanın amacı; Kuveyt Türk Yatırım Menkul Değerler A.Ş.'nin bilgi sistemlerinin ve üzerinde edinilen, saklanan, iletilen, işlenen ve yedek olarak saklanan verilerin gizlilik, bütünlük ve erişilebilirlik sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesine yönelik kural ve kontrollerle birlikte bilgi güvenliğine ilişkin süreci, rolleri ve sorumlulukları belirlemektir.

2. KAPSAM

Bu doküman, Kuveyt Türk Yatırım Menkul Değerler A.Ş'nin bilgi sistemleri ve üzerinde edinilen, saklanan, iletilen, işlenen ve yedek olarak saklanan tüm varlıkları kapsamaktadır. Politika aynı zamanda, kurum bilgi sistemleri altyapısını kullanmakta olan tüm çalışanlar, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

3. KISALTMALAR VE TANIMLAR

Bu dokümanda geçen;

a) Şirket: Kuveyt Türk Yatırım Menkul Değerler A.Ş.'yi
b) BGYS: Bilgi Güvenliği Yönetim Sistemi'ni

ifade eder.

4. SORUMLULUK

Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır.

3.1 Yönetim Kurulu

- Bilgi Güvenliği Politikasında yer alan Bilgi Güvenliği süreçlerinin, rollerinin ve sorumluluklarının gözden geçirilmesi ve aksiyonların takip edilmesinden,
- Bilgi Güvenliği Politikasının onaylanmasından,
- Güvenlik kontrol sürecini değerlendirmeye tabi tutulması ve uygunluğunun onaylanmasından,
- Bilgi güvenliği hususunda farkındalığı artıracak çalışmaların desteklenmesinden,
- Bilgi güvenliği stratejilerinin belirlenmesi ve stratejiler doğrultusunda gerekli kaynağın tahsis edilmesinden sorumludur.
- Görevler ayrılığı ilkesine uygun olarak kritik süreçlerde aynı kişi tarafından hem uygulama hem de onaylama yetkisi verilmemesinden sorumludur.

3.2 Bilgi Güvenliği Sorumlusu

- Dokümanın yılda en az bir defa ve/veya gerekli görüldüğü hallerde gözden geçirilerek güncellenmesinden,
- Varlık belirleme ve sınıflandırma çalışmasının gerçekleştirilmesi ve güncelliğinin sağlanmasından,

- BT risk belirleme ve değerlendirme çalışmasının gerçekleştirilmesi ve güncelliğinin sağlanmasından,
- Bilgi kaynaklarına yönelik tehditlerin değerlendirilmesi, ihtiyaç duyulan durumlarda aksiyonların belirlenmesi ve raporlanmasından,
- Şirket bilgi sistemleri üzerinde edinilen, saklanan, iletilen, işlenen verileri güvenlik hassasiyet derecelerine göre sınıflandırılması ve her sınıf için uygun düzeyde güvenlik kontrolü tesis edilmesinden,
- Şirket'in kendi kurumsal ağı dışındaki ağlarla iletişimde bulunduğu hallerde bu dış ağlardan gelebilecek tehditler için ağ kontrol güvenlik sistemlerini tesis edilmesi,
- Siber saldırılara karşı önlemlerin alınmasından,
- Yılda 1 kez bağımsız sızma testlerinin gerçekleştirilmesi sürecinin koordine edilmesi, aksiyonların planlaması, uygulanması ve sonuçların raporlanmasından,
- Şirket dış ağdan iç ağına yapılacak erişimleri kontrol altında tutmak amacıyla kullanılan güvenlik duvarlarının yönetilmesinden,
- Şirket çalışanlarının bilgi güvenliğine ilişkin farkındalıklarının artırılması amacıyla faaliyetlerde bulunulması ve periyodik olarak bilgi güvenliği farkındalık eğitimlerinin düzenlenmesinden,
- Bilgi güvenliğine yönelik bir olay fark ettiği an üst yönetimi bilgilendirmekten,
- Kurum içerisinde kullanılan güvenlik sistemlerinin ve gerekli görülen sunucuların işletim sistemlerinin loglarının SIEM sistemi üzerinde toplanmasının sağlanmasından ve siber güvenlik ile ilgili süreçlerde bulunan ihtiyaçlar kapsamında kural/korelasyon setlerinin oluşturulmasından,
- Kurum içerisinde yapılacak kullanıcı yetkilendirme ve erişim yetkilendirme taleplerinin mail ya da şirket bünyesinde kullanılan ITSM üzerinde bilgi güvenliği perspektifinde değerlendirilmesinden,
- Güvenlik sistemleri üzerindeki konfigürasyon, politika ve kurallarının belirlenmesi ve yürütülmesinin sağlanmasından,
- Şirket'e özgü sistem ve uygulamalar için kullanıcı kimlik ve hesap yönetimi standartlarının belirlenmesinden,
- Bilgi güvenliği olaylarına yönelik incelemenin yapılabilmesi için kritik sistem ve veri tabanları için denetim izlerini kaydederek yasal gerekliliklere uygun süreler içerisinde saklanmasının sağlanmasından,
- Şirket Bilgi Güvenliği Politikasının tüm çalışanlara duyurulması ve bilgi güvenliğine ilişkin taahhütnamelerin tüm çalışanlar tarafından imzalanması süreçlerinin tesis edilmesinden,
- Şirket bünyesinde gerçekleşen bilgi güvenliğine ait ihlallerin izlenmesi ve raporlanmasından,
- Politikanın tüm çalışanlara duyurulması, duyuru yöntemlerinin (intranet, eğitim, imza karşılığı bilgilendirme) kayıt altına alınmasından sorumludur.
- Bilgi güvenliği kontrollerinin etkinliğini ölçmek amacıyla periyodik raporlamaların yapılmasından ve sonuçlarının yönetim kuruluna sunulmasından sorumludur.

3.3 Şirket Çalışanı

- Bilgi Güvenliği Politikası ve politika ile ilgili tüm prosedürlere uyulmasından,
- Sahibi olduğu varlıklar için sınıflandırma çalışmasının gerçekleştirilmesinden,
- Varlık sınıflandırma çalışması sonucu belirlenen güvenlik kontrollerine uymaktan,
- Bilgi güvenliğine yönelik bir olay fark ettiği an Bilgi Güvenliği Sorumlusunun haberdar edilmesinden,

- Şirket kaynaklarına erişim için kullanılan her türlü hesap/parola bilgisinin saklı tutulması ve diğer Bilgi Teknolojileri çalışanları dahil hiç kimseyle paylaşılmamasından, sorumludur.

5. UYGULAMA

Bilgi güvenliği altyapısı ve organizasyonu, Şirket'in bilgi güvenliğine ilişkin temel ilkeleri ve bu konudaki ulusal yasa ve mevzuatlar ile ulusal ve uluslararası kabul görmüş standartları baz alınarak uygulanır ve geliştirilir.

1. Yürütülen tüm faaliyetlerde BGYS'nin üç ana ilkesi olan gizlilik, bütünlük ve erişilebilirliğin sürekliliğinin sağlanmasını,
2. Bilgi güvenliği faaliyetlerinin yönetilmesi, koordinasyonu ve etkin bir şekilde sürdürülebilmesi amacıyla bilgi güvenliği organizasyonu oluşturmayı,
3. Bilgi varlıklarının envanterini çıkararak sahipliklerini belirlemek, bu varlıkları sınıflandırmak, üzerlerindeki riskleri değerlendirerek gerekli kaynaklarla etkin bir şekilde yönetmek ve BGYS'nin devamlılığını sağlamayı,
4. Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren olay yönetimi faaliyetlerini yürütmeyi, ayrıca bilgi sistemlerinde gerçekleştirilen işlemlerin kayıt altına alınarak bütünlüğünün korunmasını ve mevzuata uygun sürelerle saklanmasını sağlamayı,
5. Tüm personelin BGYS'ye katılımını ve uymasını sağlamak için bilinçlendirmeyi, eğitim ve teşvikini sağlamayı,
6. Bilginin işlendiği tüm alanlarda, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla gerekli fiziksel ve çevresel güvenlik kontrollerini tesis etmeyi ve bu kontrollerin etkinliğini sürdürülebilir şekilde sağlamayı,
7. Bilgi sistemleri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirlemeyi ve hayata geçirmeyi,
8. Bilgi güvenliği gereklilikleri politikalar ile tanımlanır, tüm çalışanlara duyurulmasını ve tüm çalışanların bu politikalara uymasını sağlamayı,
9. Kurumsal iş faaliyetlerinde yaşanabilecek kesintilerin önüne geçmek, bilgiye sürekli erişimi güvence altına almak amacıyla iş sürekliliği planlarını hazırlamayı, test etmeyi ve güncel tutmayı,
10. Bilgiye erişimi yalnızca yetkili kişilerle sınırlamayı, yetkisiz erişimleri önlemeyi ve erişim kontrollerini en güvenli yöntemlerle uygulamayı,
11. Bilgi sistemleri faaliyetlerinin işletilmesinde gerekli güvenlik kontrollerini uygulamayı, bu kontrollerin etkinliğini sağlamak üzere rol ve sorumlulukları açıkça tanımlamayı,
12. BGYS politikasının iç ve dış tüm taraflara duyurulmasını, düzenli aralıklarla gözden geçirilerek güncel tutulmasını ve gerekli revizyonların uygulanmasını,
13. Bilgi güvenliği yönetim sisteminin sürekli iyileştirilmesini sağlamayı,
14. Bilgi Güvenliği Yönetim Sistemi'nin işletilmesinde istisnai ve kapsam dışı faaliyetleri de dikkate almayı ve bu kapsamda gerekli kontrolleri sağlamayı,
15. Üçüncü kişilerden hizmet alınmasının doğuracağı riskleri yönetmek, gerekli güvenlik kontrollerini tesis etmeyi,
16. 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve ilgili diğer mevzuat kapsamında çalışanlara, stajyerlere, ziyaretçilere, tedarikçilere ve ilgili diğer 3. taraflara ait kişisel bilgilerin işlenmesi, korunması ve imhası konusunda tüm sorumlulukları karşılamayı,

Taahhüt eder.

6. İSTİSNA

Bilgi Güvenliği Politikası kapsamındaki istisnai uygulamalar Üst Yönetim onayına tabidir. İstisnai durumlar için geçerli ve haklı iş gereksinimlerinin bulunması ve talepte bulunan kişi/bölümün bu istisna ile ortaya çıkan ek riski tümüyle kabul etmesi uygulamaya esastır.

7. İLGİLİ DOKÜMANLAR

P002 BGYS El Kitabı

8. YÜRÜRLÜLÜK

Doküman yayın tarihi itibariyle yürürlüğe girer.

9. REVİZYON TAKİP ÇİZELGESİ

Revizyon No	Tarih	Revizyon Nedeni	Revizyonda Yapılanlar	Revize Eden	Yeni Revizyon No
0	21.10.2025	İçerik güncelleme	BG politika ana maddeleri düzenlenmiştir.	Merve Nur KARADAŞ	1

HAZIRLAYAN / REVİZE EDEN	*KONTROL EDEN*	*ONAYLAYAN*
Kıdemli Bilgi Güvenliği Uzmanı	Üst Yönetim	Yönetim Kurulu