Tarih	YK No	Yazar	Versiyon	Açıklama
04.06.2015	2015/425	Murat Yasan	1.0	Dokümanın Oluşturulması
22.12.2020	2020/49	BT Komitesi	2.0	Dokümanın Güncellenmesi
01.12.2022	2022/40	BT Komitesi	3.0	Dokümanın Güncellenmesi

PİRAMİT MENKUL KIYMETLER A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç

Bilgi Güvenliği Politikası'nın amacı; Piramit Menkul Kıymetler A.Ş (Bundan böyle Şirket olarak anılacaktır) genelinde uygulanacak temel bilgi güvenliği prensiplerini belirlemek ve Şirket Yönetim Kurulu'nun söz konusu prensiplere verdiği desteği ve önemi ifade etmektir.

2. Kapsam

Şirket stratejik hedeflerinin desteklenmesi, sahip olunan marka değerinin korunması ve ilgili düzenlemelere uyumun sağlanması amacıyla izlenmesi gereken bilgi güvenliği kuralları ve prensipleri Bilgi Güvenliği Politikası kapsamındadır.

Bilgi Güvenliği Politikası'nın hedef kitlesi, Şirket çalışanları, Şirket mülkiyetinde veya kullanımında olan bilgi veya bilişim sistemi varlığına erişim yetkisi verilen iş ortakları, tedarikçiler ve diğer kullanıcılardır.

3. Roller ve Sorumluluklar

Rol	Sorumluluk
Yönetim Kurulu	Bilgi güvenliği gereksinimlerinin belirlenmesi amacıyla Bilgi Güvenliği Politikası'nı onaylar, söz konusu politika çerçevesinde gerçekleştirilmesi gereken faaliyetlerin takibi amacıyla Bilgi Teknolojileri Sorumlusu'nu görevlendirir.
Bilgi Teknolojileri Sorumlusu	Şirket genelinde bilgi güvenliğine yönelik, uygun güvenlik kontrollerinin uygulanması ve koordinasyonundan sorumludur.
Personel	Şirket mülkiyetinde ve kullanımında olan bilgi ve bilişim sistemi varlıklarının güncel tehditlere karşı korunması amacıyla sorumluluk alanlarına düşen görevleri yerine getirmek ve ilgili kurallara uygun hareket etmekle yükümlüdür.
İş Ortağı	Ortağı oldukları Şirket iş süreçlerinin bilgi güvenliği gereksinimlerinin sağlanması amacıyla ilgili sözleşmeler/anlaşmalar çerçevesinde hareket etmekle yükümlüdür.
Tedarikçi	Şirket iş süreçlerinin işletilmesi amacıyla ihtiyaç duyulan hizmet ve/veya kaynakların sunulmasında gerekli bilgi güvenliği gereksinimlerine uymakla yükümlüdür.

4. Bilgi Güvenliği Politikasına İlişkin Temel İlkeler

Bilgi Güvenliği Politikası; ilgili düzenlemeler ile Şirket için belirlenen görev ve sorumlulukların kesintisiz sürdürülmesi, kurum stratejik planlarının gerçekleştirilmesi, vizyon ve misyon hedeflerine ulaşılması, kurumun, çalışanların, müşterilerin ve iş ortaklarının bilgilerinin korunması amacıyla kurum bünyesinde işletilen iş süreçlerinin bilgi güvenliği kuralları ve prensipleri çerçevesinde yürütülmesini sağlar.

Şirket bünyesinde işletilen tüm iş süreçlerinin tasarımı ve işletimi aşağıda belirtilen "bilgi güvenliği" kuralları ve prensipleri çerçevesinde gerçekleştirilir.

- Şirket bilgi güvenliğinin uluslararası standartlarda yönetilmesi ve sağlanmasında bilgi güvenliği prensiplerine uyum esastır.
- Şirket iş süreçlerinin tasarım ve işletilmesinde, söz konusu süreçlerin bilgi güvenliği gereksinimlerinin belirlenmesi ve belirlenen gereksinimlerin karşılanması amacıyla etkin yöntemlerin uygulanması esastır.
- Şirket mülkiyetinde olan her türlü bilgiyi veya bilişim sistemini hedef alan bilgi güvenliği tehditlerine karşı gerekli tespit ve engelleme yöntemleri ve mekanizmaları hayata geçirilir. Söz konusu yöntem ve mekanizmaların güncel tehditlere karşı etkin koruma sağlamasını teminen gerekli güncelleme faaliyetleri yürütülür.
- Bilgi varlıklarının taşıdığı bilgi güvenliği risklerinin tamamen yok edilmesinin mümkün olmadığı ve her durumda "kalan risk" olacağı bilinci ile mevcut risklerin yönetilmesi, söz konusu kalan riski asgariye düşürecek düzeltici ve önleyici tedbirlerin etkin şekilde uygulanması esastır.
- Şirket iş süreçleri tasarımında ve işletiminde bilinen bilgi güvenliği riskleri değerlendirilerek kalan ve kabul edilenler dışındaki risklerin olasılıklarını ve etkilerini azaltıcı bilgi güvenliği kontrolleri (dokümanın devamında "kontrol" olarak ifade edilecektir) oluşturulur. Risk değerlendirme faaliyetinin ve kontrollerin etkin biçimde işletilmesi iş süreci sahibi sorumluluğundadır.
- Şirket bünyesinde üretilen, işlenen, saklanan veya iletilen her türlü bilgi Şirket mülkiyetindedir.
- Bilgi güvenliği kapsamında yürütülen faaliyetlerin hedeflenen başarıya ulaşabilmesi için kullanıcıların konuya bilinçli yaklaşımı ve sorumluluk alanlarına düşen görevleri yerine getirmesi esastır.
- Şirket çalışanlarının bilgi güvenliği farkındalığını arttırmak amacıyla yılda en az 1 (bir) defa olmak üzere "Bilgi Güvenliği Farkındalık Eğitimi" düzenlenir.
- Bilgi güvenliği konusunda bilinçli hareket etmek, bilginin güvenliğine ilişkin alınacak tedbirlerin uygulanmasına yardımcı olmak, şüpheli durumlar ile ilgili bildirimde bulunmak, iş sürekliliği faaliyetlerine destek vermek kullanıcıların görev tanımlarının ayrılmaz parçasıdır.
- Kullanıcılar, bilişim sistemleri üzerinde kendilerine tahsis edilen kullanıcı hesap bilgilerinin gizliliğinin korunması amacıyla gerekli tedbirleri almakla yükümlü olup, kendilerine tahsis edilen kullanıcı hesapları ile yapılan işlemlerden sorumludur.
- Kullanıcılar, yetkileri çerçevesinde eriştikleri bilginin kaybolmasını, bozulmasını ve yetkisiz erişilmesini önlemeye yönelik koruyucu ve düzeltici tedbirleri almakla, bilginin emanetçisi ise tedbirleri uygulamakla yükümlüdür.
- Şirket mülkiyetinde olan bilgi veya bilişim sisteminin bulunduğu fiziksel mekânlara erişimler kullanıcıların rol ve sorumluluklarıyla uyumlu şekilde sınırlandırılır.

- Şirket mülkiyetinde olan bilgiyi ve bilişim sistemini hedef alan tüm bilgi güvenliği olayları bilgi güvenliği olay yönetimi kapsamında değerlendirilir. Yapılan değerlendirmeler neticesinde, mevcut kontrollerin güncellenmesi veya yeni kontrollerin devreye alınması faaliyetleri en kısa zamanda gerçekleştirilir.
- Şirket iş süreçlerinin kesintisiz sürdürülebilmesi amacıyla İş Sürekliliği Politikası çerçevesinde "İş Sürekliliği Yönetim Sistemi" oluşturulur ve İş Sürekliliği Politikası'nda belirtilen sıklıkta yapılan olağanüstü durum tatbikatlarıyla etkinliğini koruması sağlanır.
- Tüm personelin erişimini sağlamak amacı ile politika dokümanı ve ilgili diğer dokümanlar şirket dosya dizini üzerinden ulaşılabilir hale getirilir veya periyodik olarak personele gönderilir.
- Bilgi Güvenliği Politikası, Şirket çalışanlarına duyurulduğu tarih itibarıyla tebliğ edilmiş sayılır.
- Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla müşteri ve personel bilgilerinin gizliliği sağlanır.
- Bilginin bütünlüğünü koruyacak ve sürekli erişilebilirliğini garanti altına alacak altyapıyı ve kontrolleri hayata geçirilir.
- Tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde onay mekanizması tesis edilir.
- Geliştirme, test ve üretim ortamlarının fiziksel ve /veya mantıksal olarak ayrılmasını sağlanır.
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetki verilmesi ve yetkilerin düzenli olarak kontrol edilmesi sağlanır.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliği tesis edilir.
- Hassas ödeme verilerinin ve kişisel bilgilerin iletilmesinde ve saklanmasında şifreleme, maskeleme gibi güvenliği sağlayacak tedbirlerin alınmasını sağlanır.
- Kullanılan şifreleme anahtarlarının güvenilirliği sağlanır.
- Bilgi varlıkları envanteri çıkarılır, sahipleri belirlenir ve bilgi varlıkları üzerindeki riskleri kabul edilebilir seviyeye indirmek için gerekli eylemler planlanır.
- Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren bilgi güvenliği olay yönetimi faaliyetleri gerçekleştirilir.
- Bilginin alındığı, işlendiği, saklandığı ve iletildiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemleri alınır.
- Bilgi sistemleri edinim, geliştirme bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirilir.
- Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarına ilişkin yazılı taahhüt alınır.
- Temiz masa ve temiz ekran prensibi benimsenir.
- Kullanıcı bilgisayarlarına Bilgi Teknolojileri Sorumlusu tarafından belirlenen ve kullanıcı bilgisayarlarına yüklenmiş olan yazılımlar haricinde yazılım yüklenemez.
- Taşınabilir aygıtlar yalnızca iş amaçlı olarak kullanılır. Söz konusu cihazların kullanımı, yetkilendirilmiş şahıslar tarafından gerçekleştirilse dahi; işle ilgili olmayan verilerin dağıtımında kullanılamaz.
- Kurum verilerinin, kurum içerisinde ve dışında, elektronik ya da basılı olarak taşınması, verinin gizlilik derecesine göre, taşındığı ortama ve taşıyan kişinin yetkisine bağlı olarak sınırlandırılmıştır. Çalışanlar verilerin taşınmasına yönelik olarak belirlenmiş olan güvenlik kurallarına uymalıdır.

- Mevzuat ve iş ihtiyaçlarına uygun olarak yedekleme süreçleri işletilmelidir.
- Kurumsal anti-virüs yazılımı tüm son kullanıcı bilgisayar sistemlerine yüklenir ve virüslere, Truva atlarına, solucanlara, casus yazılımlara, reklam yazılımlarına veya rootkit'lere karşı koruma sağlanır.
- Log kayıt sistemi ve yedekliliği düzenli olarak kontrol edilmelidir.
- Oluşabilecek olağan üstü durum tanımları farklı senaryolarla birlikte değerlendirilmeli, Kurum verilerinin ve iş sürekliliğinin sağlanması için, bu senaryolar karşısında alınacak tedbirler ve aksiyon planları belirlenmelidir.
- Bu tedbirler güncel şartlar ve teknolojik değişimler göz önüne alınarak her yıl düzenli olarak gözden geçirilmelidir.
- Oluşturulan yedek merkeze kritik bilgilerin yedeklenmesi ve oluşabilecek olağanüstü bir durumda sistemin hızlı bir şekilde çalışır hale getirilmesi hedeflenmelidir.

5. Bilgi Teknolojisi Sorumlusunun Bilgi Güvenliği Hususlarına İlişkin Sorumlulukları

- Bilgi Güvenliği Yönetim Süreci'nin kurulumuna yönelik yapılan çalışmaları organize eder ve yapılan çalışmalar hakkında yönetimi bilgilendirir,
- BS risk değerlendirme çalışmalarını koordine eder,
- Gerekli politika, prosedür ve dokümanların oluşturulması çalışmalarını koordine eder,
- Bilgi Güvenliği projelerinin hayata geçirilmesi çalışmalarını koordine eder,
- Yeni başlatılan veya devam eden projelerde bilgi güvenliğine yönelik gereksinimleri belirler,
- Açıklık analizi çalışmalarını koordine eder,
- Bilgi güvenliğinin izlenmesine yönelik faaliyetleri koordine eder,
- Bilgi Güvenliği Yönetim Süreci'ne yönelik farkındalığın artırılması amacıyla eğitim ve bilgilendirme faaliyetlerinin gerçekleştirilmesini sağlar,
- Bilgi Güvenliği Yönetim Süreci politika ve prosedürlerinin güncel kalmasını sağlar,
- Bilgi güvenliğini etkileyen, iç ve dış mevzuata uyum çalışmalarını koordine eder,
- Bilgi Güvenliği Politikasının herkese bildirilmesi ve uygulanması için gerekli mekanizmaların kurulmasını sağlar,
- Bilgi güvenliğine yönelik eğitim ihtiyaçlarını belirler,
- Meydana gelen atakların takip edilmesini, gerekli önlemlerin alınmasını ve raporlanmasını koordine eder,
- Bütçe hazırlama döneminde güvenlik ile ilgili bütçenin hesaplanmasına destek verir,
- Bilgi varlıklarına ait risklerle ilgili konularda gerektiğinde üst yönetim ve yönetim kuruluna danışmanlık yapar.
- Geliştirilen yazılımlara yönelik güvenlik standartlarını belirler,
- Bilgi Güvenliği Politikasını yılda en az bir kere gözden geçirir ve güncellenmesi durumunda üst yönetimin onayına sunar.
- Merkezi log kayıt sisteminin düzenli olarak takibi ve raporlamasını yapar,
- Yedek merkezin her zaman hazır ve güncel durumda kalmasını sağlamak için gerekli kontrolleri yapar.

6. Bilgi Güvenliği Politikasının Gözden Geçirilmesi

Şirket Bilgi Güvenliği Politikası Bilgi Teknolojileri Sorumlusu tarafından yılda en az bir kere gözden geçirilir ve gerekli görülmesi durumunda güncellenerek üst yönetim onayına sunulur. Güvenlik teknolojilerindeki gelişmelere bağlı olarak ortaya çıkan ihtiyaçları içerecek yeni politikalar üretilir.

7. Yürürlük

Bilgi güvenliğine ilişkin bu düzenleme, üst yönetimin aşağıda yazan onay tarihi itibariyle yürürlüğe girer. Şirket'in bilgi güvenliğine ilişkin tüm uygulama ve iş akışları politika hükümleriyle uyumlu şekilde oluşturulur/güncellenir.

Bu Prosedür Piramit Menkul Kıymetler A.Ş. Yönetim Kurulu'nun 01/12/2022 tarih ve 2022/40 sayılı kararı ile yürürlüğe girmiştir.

Yönetim Kurulu Başkanı
Mehmet OSMANOĞLU

Yönetim Kurulu Bşk. Vekili
Zekiye YOLCUBAL

Yönetim Kurulu Üyesi
Nurşen OSMANOĞLU

Yönetim Kurulu Üyesi
Sudi AYDEMİR

Yönetim Kurulu Üyesi
Mine Berra DOĞANER