1. AMAÇ

Bilgi Güvenliği Politikası'nın amacı InvestAZ Yatırım Menkul Değerler A.Ş.'nin iş sürekliliğini sağlamak ve potansiyel tehditlerin etkisini azaltmak için bilgi güvenliği olaylarını engellemek veya hasar riskini minimize etmektir. Bilgi; iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. Kurumsal bilginin Gizlilik, Bütünlük, Kullanılabilirlik ile ilgili ortaya çıkabilecek riskleri ve bu risklerin etkilerini en aza indirmeyi amaçlar. Kurum faaliyetlerimiz esnasında hizmet vermekte olduğu müşterilerinin özel erişim/bağlantı bilgilerine, kritik cihazlara ait özel parola, ayar ve iletişim bilgilerine sahip olabilmektedir.

2. KAPSAM

Bu politika, InvestAZ Yatırım Menkul Değerler A.Ş. bünyesindeki bilgi varlıklarını kapsamaktadır. Hizmet verilen kurum ve kuruluşların güvenini temin etmek ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliğini sağlamamız öncelikli amacımızdır.

3. SORUMLULUK

Bilgi Güvenliği, Yönetim Kurulu kapsam çerçevesinde kurumun bilgi varlıklarına yönelik risklerin üst yönetim tarafından onaylanan kabul edilebilir seviyede tutulmasından sorumludur.

4. POLİTİKA

Bilgi Güvenliği Politikası bağlamında; iş birliğinde bulunduğumuz müşteriler, resmi kurumlar ve irtibat bürolarımız ile ilişkilerimiz çok değerlidir. Sunmakta olduğumuz hizmetlerin sürekliliği, elimizde tuttuğumuz bilgilerin gizliliği, müşterilerin veya kendi içimizdeki bilgi varlıklarının bütünlüğü yüksek öneme sahiptir.

Bu amaçla :

- Politikanın hedefi şirketin bilgi varlıklarını iç ve dış kasıtlı veya kasıtsız tehditlere karşı korumaktır.

- Risklerimizi sürekli gözden geçirip ve kabul edilebilir seviyenin üstündeki riskler için kontroller uygulamaktadır. Bilgi Güvenliği Risk Analiz Prosedürü ve Risk Analiz Şemasında belirlenmiş riskleri kontrol altında tutmak için Bilgi Teknolojileri Yetkilisinin vermiş olduğu bildirimlere göre Bilgi Güvenliği Sorumlusu tarafından ilgili kontroller yapıldıktan sonra gerekli bildirimler üst yönetimle paylaşılıp aksiyon alınması hedeflenmektedir.

- Bilgi Güvenliği Politikası aşağıdaki tüm gereksinimleri güvenceye almasını sağlamaktadır:

  - Süreçler ve bilgi varlıklarının tanımlanması ve bunlarla ilgili risk değerlendirmelerinin metodolojik olarak gerçekleşmesi
  - Bilgilerinin ve bilgi sistemlerinin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanmasını
  - Bilginin yetkisiz erişimden korunması
  - Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini
  - Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi
  - Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirmeyi ve çalışmalarını gerçekleştirmeyi
  - İş süreçlerinin ihtiyaç duyduğu her anda bilgiye erişimin mümkün olması
  - Yasal yükümlülüklerin ve sözleşmelerden doğan hukuki yükümlülüklerin yerine getirilmesi
  - İş sürekliliği planlarının geliştirilmesi ve iyileştirilmesi

- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi
- Tüm Bilgi Güvenliği ihlallerinin veya ihlal şüphesinin bilgi güvenliği Yönetim Kurulu'na bildirilmesini ve incelenmesinin sağlanması
- Kurumun tüm ağ güvenliğinin, görevler ayrılığı prensibinin, işlemlerin kayıtların ve verilerin bütünlüğünün, dış kaynak yoluyla alınan hizmetlerin, müşteri bilgilerinin gizliliğinin, varlık yönetimlerinin ve kontrollerinin sağlanmasına yönelik çalışma sağlanması

Kurumun Bilgi Güvenliği Politikaları, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, Kurum bilgilerini veya iş sistemlerini kullanan tüm Kurum personeli için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve Kurum bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

- Bu politikayı desteklemek için prosedürler ve bunlara bağlı talimatlar tanımlanmıştır.

- Çalışanlarımızın bilgi güvenliği bilinçlerini yüksek tutmak için çalışmalar yapılması sağlanmaktadır.

- Bilgi Güvenliği iş ihtiyaçları gözetilerek sağlanmaktadır.

- Bilgi Güvenliği, Yönetim Kurulu bu politika ve buna bağlı tüm dokümanların, Bilgi Yönetim Sistemi'nin geliştirilmesi, dokümante edilmesi ve sürekli iyileştirilmesi sağlanmaktadır.

- Tüm yönetim kadrosu yönetmekte oldukları birimlerin bu politika ve buna bağlı prosedürlere uymasından sorumludur.

- Bilgi Güvenliği Politikasına uyumluluk tüm çalışanlar için zorunludur;

Bilgi Güvenliği'nin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; Kuruma ait bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması; ve bilgilerin ve sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm Kurum ve dış kaynaklı personel ile stajyerleri ve irtibat bürosu personeli konumları veya görevleri ne olursa olsun işlerini, bilgilerin Kurum bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur. Kuruma ait bilgilerin eksiksiz, doğru ve kullanılabilir durumda hazır olmasının sağlanmasının yanı sıra tüm Kurum personeli, Kurum Personel Yönetmeliği Kurallarında belirtilen gizli bilgilerin korunması ve Kurum İş Ahlakı İlkelerine de uymak zorundadır. Kurum; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve InvestAZ Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmayı taahhüt eder.

- Bu politikayı yılda bir kez gözden geçirerek güncel tutmaktayız;

Bilgi Güvenliği politikaları Kurum bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtması amacıyla yapılan varlık ve risk güncellemelerine paralel olarak yılda en az bir defa gözden geçirirler. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları yeni gerekli eklemeler yapılarak güncellenir. Ayrıca herhangi bir Kurum çalışanı Bilgi Güvenliği Politikaların gelişmesi ve

Kurum'un ihtiyaç duyduğu kontrolleri daha iyi yansıtması amacıyla politikaların değiştirilmesi konusunda Bilgi Teknolojileri ve Bilgi Güvenliği Sorumlusu'na talepte bulunabilir. Yapılan talepler Bilgi Teknolojileri ve Bilgi Güvenliği Sorumlusu tarafından ele alınır ve değerlendirilir.

Bilgi Güvenliği Politikası ilkeleri, Kurum İnsan Kaynaklarının Personel Yönetmeliği Kurallarına paralel uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

5. DENETLEME VE POLİTİKALARA UYULMASI VE UYULMAMA DURUMLARININ ÇÖZÜMLENMESİ

Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derece sorumludur. Bilgi Teknolojileri Yönetişimi ve Bilgi Güvenliği Sorumlusu başta Bilgi Güvenliği Ana Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur. Bilgi Güvenliği Politikası ihlalleri, Kurumun risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda Kurum Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim, gerek denetim, gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri istihdama son verilmesine hatta Adli ve Cezai yasal işlemler başlatılmasına varıncaya kadar gidebilecek şirket içi disiplin cezaları ile sonuçlanabilecektir. Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.

6. POLİTİKA HEDEFLERİ

Kurum Bilgi Güvenliği, Kurum'un itibarının, güvenilirliğinin, bilgi varlıklarının korunması, temel ve destekleyici iş faaliyetlerinin mümkün olan en az kesinti ile devam etmesi amacıyla,

- Bilgi sistemlerinin sürekliliğini tam olarak sağlamayı,
- Çalışanların bilinç, farkındalık ve güvenlik gereksinimlerine uyum düzeylerini en üst seviyeye çıkarmayı,
- Üçüncü taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,
- Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi,
- Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve saklanmasını,
- En güncel ve etkin teknik güvenlik kontrolleri uygulamayı hedefler.

Her bir Kurum çalışanı bu hedeflere katkı sağlamaktan sorumludur.