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. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi İşlem Ekibi ve Yönetim Temsilcisi olarak Bilgi Güvenliği Sorumlusu (BGS) tarafından işlemler yürütülmektedir. BGS ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır. Kapsam içindeki departmanlardan BGS temsilcileri belirlenmiştir. BGS ekip üyesi olarak isim bazında atamaları yapılmıştır.

3.1. Yönetim Sorumluluğu

- Şirket Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder.
- BGYS kurulumu sırasında Bilgi Güvenliği Sorumlusu Yönetim Temsilcisi atama yazısı ile atanır. Gerekli olduğu durumlarda üst yönetim tarafından doküman revize edilerek atama tekrar yapılır.
- Yönetim kademesindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan anlayış, kurumun en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden tüm yöneticiler yazılı ya da sözlü olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.
- Üst Yönetim, Bilgi Güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

3.2. Yönetim Temsilcisi Sorumluluğu

- BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesini,
- BGYS kurulumunda destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın

oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,
- BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,
- İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile BGYS ve kontrollerin değerlendirilmesi,
- BGYS'de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

3.3. Bilgi İşlem Ekip Üyeleri Sorumluluğu

- Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,
- Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisini (BGS) bilgilendirmesi,
- Birim çalışanlarının politika ve prosedürlere uygun çalışmasını sağlanması,
- Bölümleri ile ilgili BGYS kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,
- BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

3.4. İç Denetçi Sorumluluğu

İç denetim planı doğrultusunda, görev verilen iç denetimlerde denetim faaliyetlerinin yapılmasından ve raporlanmasından sorumludur.

3.5. Birim Yöneticilerinin Sorumluluğu

Bilgi Güvenliği Politikasının uygulanması ve çalışanların esaslara uymasının sağlanmasından, 3. tarafların politikadan haberdar olmasının sağlanmasından ve fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden sorumludurlar.

3.6. Tüm Çalışanların Sorumluluğu

- Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve bilgi güvenliği yönetim sistemi dokümanlarına uygun olarak yürütmekten,
- Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapar ve hedeflere ulaşılmasını sağlar.
- Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan,
- Üçüncü taraflar ile yapılan ve satın alma sorumluluğunda olmayan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

3.7. Üçüncü Tarafların Sorumluluğu

Bilgi güvenliği politikasının bilinmesi ve uygulanması ile BGYS kapsamında belirlenen davranışlara uyulmasından 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 uygulanmaktadır. Bilgi Güvenliği Risk Yönetim 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 bunlara 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, politikalar ve bunlara bağlı talimatlar tanımlanmıştır.

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

- Bilgi Güvenliği iş ihtiyaçları gözetilerek ilgili aksiyonlar hedeflenmektedir.

- Bilgi Güvenliği kapsamında, üst yönetim bu politika ve buna bağlı tüm dokümanların, Bilgi Yönetim Sistemi'nin geliştirilmesi, dokümante edilmesi ve sürekli iyileştirilmesi için çalışmalar yapılmasını sağlamaktadır.

- 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; bilgilerin ve sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm Kurum ve dış kaynaklı personel, stajyerler 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 Etik Davranış Kuralları ve Uygulama Prensipleri'ne de uymak zorundadır. Kurum; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve InvestAZ Kişisel Verilerin Korunması Politikası'na 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. GİZLİ BİLGİ NEDİR?

InvestAZ Yatırım Menkul Değerler A.Ş. muhasebe kayıtlarında yer almasa dahi bilgi, değerli ve kritik bir girdi olduğundan önemli niteliktedir. Kurum çalışanlarına sadece işlerini icra edebilmeleri için verilen gerekli bilgiler, çalışanlarca bilinen müşteri/personel bilgileri, ticari sırlar, sözleşmeler ve Kurum içerisinde paylaşılan her türlü bilgi gizli bilgidir.

6. BİLGİ GÜVENLİĞİ POLİTİKA ESASLARI

Çıkar çatışması politikasının uygulanmasından, Kurum nezdinde görev alan her personel, gözetiminden ise yöneticiler sorumludur. Bu kapsamda Kuruma, müşterilerine, ilişkili olduğu kurumlara ait bilgilerin güvenliği yüksek önem taşır. Kurumun sunmuş olduğu faaliyetler çerçevesinde; personelin görev aldığı birime ilişkin yürürlükte olan iş akışları, görev tanımları, Kurum içerisinde yayınlanmış her türlü duyuru, bilgi, belge vesaire dokümanlar doğabilecek

herhangi bir çıkar çatışmasında yol gösterici niteliğe haiz olup, bilgi güvenliği politikası çerçevesinde gizli tutulur.

- **Alım – Satım Aracılığı Kapsamında Bilgi Güvenliği**

  Sermaye Piyasalarında alım satım gerçekleştiren müşterilerin hizmet şartları, Kurum yönetimi ve/veya Kurum kredi komitesi tarafından analiz, bilgi ve belgelere dayandırılarak belirlenir, bu doğrultuda fırsat eşitliği unsuru ihlal edilemez ve müşteri bilgileri paylaşılamaz. Bahsi geçen belgelerin saklanması ilgili birim nezdinde yapılır.

- **Yatırım Danışmanlığı Faaliyeti Kapsamında Bilgi Güvenliği**

  Kurum ve Kurumu temsil eden kişiler tarafından sunulan yorum ve tavsiyelerin güvenilir kaynak, belge, rapor ve analizlerle desteklenmesi zorunludur. Ancak müşterilerin yatırım kararlarını etkileyebilecek nitelikte olan araştırma sonuçları, müşterilere duyurulmadan önce kurum, personel veya üçüncü şahısların lehine kullanılamadığı gibi gizli nitelik taşır ve paylaşılmaz.

- **Halka Arza Aracılık ve Danışmanlık Faaliyetleri Kapsamında Bilgi Güvenliği**

  Kurum, halka arz sürecinde kamuya açıklanmamış bilgilerin, halka arza aracılık faaliyetlerini yürüten birim dışındaki yetkisiz birimlerle ve kurum dışındaki yetkisiz kişilerle paylaşılmasını engellemek amacıyla gizlilik sözleşmesi düzenler ve gerekli tedbirleri alır. Bu bağlamda bilgileri kapsayan belgelerin saklanması, ilgili birimler nezdinde yapılır. Kurum ile yatırımcı arasında eşit mesafede bulunularak, iki tarafın haklarını dengeli olarak gözeten birim, başka kurum ve hatta InvestAZ Yatırım Menkul Değerler A.Ş. içerisinde paylaşılmaması gereken birim ile bilgiyi paylaşamaz.

- **Saklama Hizmeti Faaliyeti Kapsamında Bilgi Güvenliği**

  Kurum, saklama hizmeti sunulması sırasında veya Kurum faaliyetleri neticesinde müşteriye ait edinilen bilgilerin, müşteri çıkarlarına aykırı olarak kurum dışında ve kurum içerisinde farklı birimler arasında paylaşılmasını engeller. Müşteri hesaplarına ilişkin bilgilerin gizliliği esastır. Ancak müşterinin bilgilendirilerek SPK mevzuatı kapsamında yetkili kılınan taraflara bilgi verilmesi, gizliliğin ihlali sayılmaz.

- **Diğer Sermaye Piyasası Faaliyetleri Kapsamında Bilgi Güvenliği**

  Kurum, Sermaye Piyasası Kurulu tarafından faaliyet izni verilmiş diğer Sermaye Piyasası Faaliyetleri kapsamında faaliyetlerini icra ederken, müşterilere ait bilgilerin gizliliğini esas alır ve gerekli bilgi güvenliği tedbirlerini uygular.

7. ÖNLEMLER

- **Bilgi Güvenliğinin Sağlanması**

  Müşterilerin, personelin ve Kurumun iş yaptığı üçüncü tarafların şahsi ve mali bilgileri iş amacı dışında kullanılamaz. Kurum personeli, işleri gereği öğrendikleri bilgileri ve haiz oldukları belgeleri (müşteri bilgileri, proje, teknik altyapı, yönetmelik, özlük hakları vb. dahil) Kurum içindeki ve dışındaki yetkisiz kişi ve/veya mercilerle paylaşamaz.

Her türlü doküman, bilgi veya araçların izni verilen ve kurumdaki görevin gerektirdiği durumlar haricinde, kişisel ve özel çıkarlar için veya üçüncü şahıslar, kurum ve kuruluşlar yararına, çalışılan süre içinde veya daha sonrasında kullanılması kesinlikle yasaktır.

Kurum, nezdinde kullanılan tüm verilere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Yetkilendirme düzeyi ve erişim haklarının atanmasında görev ve sorumluluklar göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

Görevler ayrılığı ilkesi ile bilgi sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanları ayrılır. Bu şekilde kritik işlemler tek bir personele bağımlı olmayacak şekilde tasarlanır. Kurum bilgi sistemleri üzerindeki bilgilerin güvenliği amacıyla log kayıtları düzenli olarak tutulur. Kurum personelinin sisteme, otomasyon ve diğer elektronik platformlara erişiminde bireysel giriş şifrelerinden oluşan şifreler kullanılır. Bilgi sistemlerinde yer alan kullanıcı kimliği, şifreler, elektronik imza ve sertifikalar kişiye özeldir ve kimseyle paylaşılamaz.

- **Bilgi Paylaşımı**

Personelin olası bilgi güvenliğini ihlal etmesini engellemek amacıyla kendisi veya yakınları lehine çıkar çatışması ya da izlenimi yaratacak durumlara sebebiyet vermemesinden kaçınılır, kendisinin veya yakınlarının menfaatlerini ilgilendiren konularda karar sürecinde yer almaz, hesap sahibi haricinde bir kimse ile müşteri bilgileri, hesabında ilişkin detay vesaire bilgileri paylaşılamaz.

Personel, Kurum organizasyon şemasında belirlenen yapıda ve ilgili mevzuat ve usuller çerçevesinde yetkilendirilip görevlerini yerine getirirler.

- **Şirket Dışı Görev Alma**

Kurum, personelinin Kurum içi sorumluluklarını ihmal etmesine sebep olmayacak, Kurum ve Müşteri çıkarlarına uygun hareket etmesini kısıtlamayacak, Etik Davranış ve Uygulama Prensipleri'ne uyum içerisinde olan kurum dışı faaliyetlerde bulunmasını engellemez. Ancak bu tür faaliyetlere katılan personel, Kurum içerisinde edindiği bilgiyi paylaşmaz.

- **Çalışma Alanları**

Çalışma alanları, sadece görevin icra edildiği çalışma masasından ibaret olmayıp, toplantı odaları, bütün çalışanların kullandığı ortak alanlar, faks, yazıcı, gibi elektronik cihazların olduğu alanlar da bu alan içerisine girer.

Mesai saatleri içeresinde çalışanlar, masalarında başka bir çalışanın görmemesi gereken bilgi ve belgeye ait evrakı, masalarında görülmeyecek şekilde muhafaza eder. Mesai saatleri dışında ise faks, yazıcı gibi elektronik cihazlarda herhangi bir çıktının olup olmadığının kontrolü, her çalışanın kendi sorumluluğu altındadır. Bilgilerin içerisine ait evraklar, bütün çalışanların ortak kullandığı alanlarda bulunmaz.

Kurum içi üretilen rapor ve belgeler gizlilik sınıfına göre dosya sunucusu üzerinde kişisel klasörlerde, birim ortak klasöründe ve/veya ilgili birimlerin ortak klasörlerinde saklanır.

Kurum dışı gelen evrak ve belgeler ilgili birim tarafından kayıt altına alınır ve ilgili birim/birimler veya personele yönlendirilir.

Kurum iç ve dış e-posta trafiği kayıt altına alınır.

Kurum müşterileriyle gerçekleşen telefon görüşmeleri kayıt altına alınır.

- **Bilgi Sistemleri Çerçevesinde Alınan Önlemler**

  - Sunucu ve aktif cihazların bulunduğu sistem odasına yetkili personelin girişleri kayıt altına alınır.
  - Sunuculara, ağ ve aktif cihazlara erişim, Bilgi Teknolojileri personeli tarafından sadece yetkili olduğu sisteme, sahip olduğu kullanıcı adı ve şifre ile erişim yapabilir.
  - Her bir program kullanımı içi personele ayrı ayrı kullanıcı adı ve şifre oluşturularak yetkiler dahilinde programda yapabileceklerine izin verilir.
  - İnternet üzerinden işlem yapan müşterilerimiz sisteme, müşteri bilgileri veya güvenlik adımlarını geçtikten sonra erişim sağlayabilir.
  - Personelin sisteme girişi, kullanılan programlara logini veya yapılan işlem hareketleri sürekli olarak loglanır ve düzenli olarak backupları alınır.
  - Tüm ağ sisteminde olan hareketler programlar aracılığıyla loglanır.
  - Müşterinin hangi internet protokolü numarası ile sisteme bağlandığı, ne zaman bağlanıp ne zaman sistemden çıktığı, yaptığı işlemler, hangi menülere girdiği gibi tüm hareketler loglanır.
  - Kurumlar ile kurulan sanal ağ bağlantısı loglanır.
  - Kurum yerel ağı, İnternet, DMZ (Bağlantılardan arındırılmış bölge), bağlantı sistemleri, kurumlar arasında Vsanal özel ağ gibi birçok ağdan oluşur ve tüm bu ağlar arasındaki geçişler firewall olarak adlandırılan güvenlik ihlallerine karşı alınacak müdahale hakkında bilgi oluşturulur.
  - Firewall sistemi üzerinde oluşturulan kurallar ile yetki çerçevesinde, sistemlere veya kişilere erişim sağlanır ve ilave sistemler ile güvenlik seviyesi üst seviyeye çıkarılır.
  - Tüm bu ağları ve farklı ağları birbirine bağlamak için yönlendiriciler kullanılır. Yönlendiriciler üzerine yazılmış ağ kuralları ile güvenliğin artırılması sağlanmış, internet şubesinde gerçekleşen işlem trafiğinin dinlenilmemesi için güvenli soket katmanı ile önlem alınmıştır.
  - Yönlendiriciler ve/veya firewall üzerinde yazılan erişim yetkisi sayesinde izin verilmeyen kişi ve sistemlerin erişimi engellenmiştir.
  - Kurum ağ sistemini içeriden ve dışarıdan gelebilecek saldırılara ve ataklara karşı korumaya almıştır. E-posta ve transfer yolu ile gelebilecek saldırılara karşı koruma ve engelleyici önlemler mevcuttur. Ayrıca firewall üzerinde bulunan saldırı tespit ve engelleme sistemleri yardımı ile güvenlik sağlanır.
  - İçeriden gelebilecek saldırılara karşı tüm bilgisayarlar ve sunucular, merkezi virüs yönetimi sistemi ile yönetilir. Virüs veritabanı güncellemeleri düzenli olarak yapılarak, olası problemler hakkında eş anlı olarak Bilgi Teknolojileri Birimi'ne ve ilgili Birim'lere e-posta gitmekte ve izleme programı aracılığıyla canlı izleme yapılmaktadır.
  - Tüm sistemler düzenli olarak yedeklenerek sistemin sürekliliği sağlanmakta olup, alınan yedekler Bilgi Teknolojileri Yedekleme Prosedürü çerçevesinde yürütülür.
  - Oluşan hatalar, ihlaller, güvenliği sarsacak ya da sistem sürekliliğini tehdit edecek durumlarda Bilgi Teknolojileri Birimi Yetkilisi yetkisi çerçevesinde gereken müdahaleyi yapar. Giderilen sorun hakkında ilgili kişi ya da birimin (sorunun birime ne şekilde ulaştığına bakılarak, kullanıcının bilgi ihlal prosedürüne göre açtığı ihlal kaydını kullanarak) ilgili kanal aracılığı ile haberdar olması sağlanır.
  - Kurum içi üretilen rapor ve belgeler gizlilik sınıfına göre dosya sunucusu üzerinde kişisel klasörlerine, birim ortak klasörüne ve/veya ilgili birimlerin ortak klasörlerinde saklanır.

8. 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.

9. 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.