1. AMAÇ

Kuruluşumuzun yönetim anlayışı ile öncelikli amacımız; hizmet verilen kurum ve kuruluşların güvenini temin etmek ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliğini sağlamaktır. Bu bağlamda; iç paydaşlarımız ve dış paydaşlarımız ile kurduğumuz ve yürütmekte olduğumuz ilişkilerimiz çok değerlidir. Sunmakta olduğumuz ürün ve hizmetlerin sürekliliği, elimizde tuttuğumuz bilgilerin gizliliği, müşterilerin veya kendi içimizdeki bilgi varlıklarının bütünlüğü en yüksek öneme sahiptir.

Bilgi Güvenliği ile ilgili olarak hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetimin yaklaşımını tanımlamak, tüm çalışanlara ve ilgili taraflara bu yaklaşımı bildirmektir.

2. KAPSAM

Bu politika; Kuruluşumuzun bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans, kalite güvence, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullanılan bilgi güvenliği süreçlerinin tamamını kapsar.

İç Kapsam (İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;)

- Kuruluş üst Yönetimi bünyesindeki tüm departmanlar ve çalışanlar,
- Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar,
- Kuruluşumuza ait fiziksel çalışma alanları,
- Kullanılan yazılım ve donanımların yapısı ve ekipmanlar,
- Çalışanların risk ve fırsat değerlendirmelerine katılım yöntemleri,
- İSG-Ç Hedefleri ve Çalışmaları,
- Yerine getirilecek politikalar, prosedürler, hedefler ve stratejiler;
  - → Bilgi Güvenliği Yönetim Sistemi Politikası,
  - → Tüm Bilgi Güvenliği yönetim sistemleri prosedürleri,
  - → Yönetimce belirlenmiş yıllık Bilgi Güvenliği yönetim sistemleri hedefleri,
  - → Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),
  - → Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için yönetim tarafından atanan Yönetim Temsilcileri ve Bilgi Güvenliği Yönetim Sistemi ekibi,
  - → İç paydaşlarla ilişkiler ve onların anlayışları ve değerleri, kuruluşun kültürü, kuruluş tarafından uygulanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini

kapsamaktadır.

Dış Kapsam

- Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,
- Ulusal ve Uluslararası Rekabet Hukuku, Politikaları ve Prosedürleri,
- Tedarikçi ve müşteri verilerinin gizliliği,
- Kalite Odaklılık,
- Kuruluşun hedefleri üzerinde etkisi bulunan paydaşlarla ilişkiler ve onların anlayışları ve değerleri;
- İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,
- TSE ve diğer kuruluşlarla olan ürün belgelendirmeleri,
- Teknolojik Yeniliklere Ayak Uydurmak,
- Tedarikçiler,
- Doğal afetler, enerji kesintileri, siber saldırılar

3. SORUMLULUKLAR

Bilgi Güvenliği Yönetim Sistemi (BGYS) Politikası ile bu politika ışığında tanımlanan diğer dokümanlarda kişilere verilen sorumlulukların kapsamı aşağıdaki tabloda belirtilmiş olup, yayın tarihinden sonra hazırlanan yeni bir dokümanda yeni bir sorumlu/sorumluluk belirlenmesi durumunda oluşturulan politikanın içerisinde tanımlama yeni bir tanımlama yapılır ve sorumlunun görev tanımı buna göre revize edilir.

Sorumlu(lar)	Sorumluluk(lar)
Yönetim	● Kuruluş Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan BGYS'ne uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlanacağını taahhüt eder. ● Yönetim kademesindeki yöneticiler güvenlik konusunda kendisinden alt kademelerde bulunan personele görev verme yanında örnek olma açısından da sorumludur. Üst kademelerden başlayan ve uygulanan bu anlayışın, firmanın en alt kademe personeline kadar inmesi 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 kapsamında olan çalışmalar için gerek duyulan bütçeyi oluşturmakla yükümlüdür.

Sorumlu(lar)	Sorumluluk(lar)
Üst Yönetim Temsilcisi	● BGYS Üst Yönetim Temsilcisi; BGYS kurulumu sırasında atama yazısı ile atanır. Yönetim temsilcisinin işten ayrılması veya herhangi bir sebeple temsilcide değişiklik yapılması gereken durumlarda ise doküman revize edilerek atama üst yönetim tarafından atama tekrar yapılır. Üst Yönetim Temsilcisinin Sorumlulukları aşağıdaki şekilde sıralanmıştır: ● BGYS Ekibine Liderlik Etmek, ● BGYS Ekibini seçmek, seçilen ekip için hazırlanan atama evraklarını onaylamak, ● BGYS Çalışmalarına Üst Yönetim adına önderlik etmek, ● BGYS 'de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanması çalışmalarını gözden geçirmek, onaylamak ve Yönetim Kurulu'na sunmak, ● Kriz zamanlarında Yönetim Kurulu üyelerine ulaşamadığında süreci Kuruluş lehine yürütmek adına kararlar almak, ● BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin, risk ve fırsat analizlerinin sürekliliğinin sağlanması için yetkin kişileri görevlendirmek, ● BGYS ve KYS çalışmaları kapsamında hazırlanan ve hazırlanacak tüm dokümanları (el kitabı, politika, prosedür, varlık yönetimi, süreç, akış şemaları, talimat, plan, formlar, listeler, tutanak, kılavuz vb.) gözden geçirerek Yönetim Kurulu son onayından önce nihai olarak onaylamakla yetkilidir.
BGYS Yönetim Temsilcisi	● BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesi, ● 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 ve fırsat değerlendirmelerinin sürekliliğinin sağlanması,

Sorumlu(lar)	Sorumluluk(lar)
	● İç denetimlerin yürütülmesi, hedeflerin ve yönetim gözden geçirme toplantıları ile BGYS ve kontrollerin değerlendirilmesi, ● BGYS'de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından, ● BGYS Ekibine önderlik etmekten sorumludur.
BGYS Ekip Lideri	BGYS Ekip Lideri; ● BGYS Ekip üyelerinin sorumluluklarına ek olarak, ● BGYS Ekibine öncülük etmekle ve ekip üyelerinin sorumluluklarını yerine getirme kontrollerini yapmakla sorumludur.
BGYS Ekip Üyeleri	BGYS Ekip Üyeleri; ● Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmaların yapılmasından, ● Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisinin bilgilendirilmesinden, ● Departman çalışanlarının politika ve prosedürlere uygun çalışmasının sağlanması ve takibinden, ● Bölümleri ile ilgili BGYS kapsamında farkındalığın oluşması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanmasından ve ● BGYS' de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.
Departman Yöneticileri	Bölüm Yöneticileri ● Bilgi Güvenliği Politikasının uygulanması ve çalışanların esaslara uymasının sağlanmasından, ● Üçüncü tarafların politikadan haberdar olmasının sağlanmasından ve fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden, ● İş tanımı değişen veya kurumdan ayrılan / ayrılacak olan kullanıcıların erişim haklarının revize edilmesi / silinmesinden Organizasyonundan sorumludur.

Sorumlu(lar)	Sorumluluk(lar)
Tüm Çalışanlar	Tüm Çalışanlar; ● Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve BGYS dokümanlarına uygun olarak yürütmekten, ● Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yaparak hedeflere ulaşılmasını sağlamaktan, ● Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan ve ● Üçüncü taraflar ile yapılan ve Satın alma sorumluluğunda olmayan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.
Üçüncü Taraflar	Üçüncü Taraflar; ● BGYS Politikasının bilinmesi ve uygulanması ile BGYS kapsamında belirlenen davranışlara uyulmasından sorumludur.

4. TANIM ve KISALTMALAR

Terim	Tanım/Açıklamalar
Kurum / Kuruluş	TURK Finansal Teknoloji A.Ş.
Bilgi Güvenliği	Bilgi, tüm diğer kurumsal ve ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun şekilde korunması gereken bir varlıktır. Kuruluş içerisinde, süreç, formül, teknik ve yöntem, müşteri kayıtları, pazarlama ve satış bilgileri, personel bilgileri, ticari, sınai ve teknolojik bilgiler ve sırlar gizli bilgi olarak kabul edilecektir.
Gizlilik	Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemesine izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Örneğin; şifreli e-posta gönderimi sırasında e-posta ele geçirilse dahi yetkisiz kişilerin içeriği okumalarının engellenmesi de bu sınıfa dahildir).

Terim	Tanım/Açıklamalar
Bütünlük	Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler ile çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Örnek: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması - elektronik imza - mobil imza)
Erişilebilirlik	Bilginin / Bilgi Varlığının ihtiyaç duyulduğu her an erişime hazır olmasıdır. Diğer bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Örnek: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şaselerinde yedekli güç kaynağı kullanımı - UPS).
Bilgi Varlığı	Kuruluşun sahip olduğu, faaliyetlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler kapsamında bilgi varlıkları şunlardır: ● Kâğıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri, ● Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım, ● Bilginin transfer edilmesini sağlayan ağlar, ● Tesisler ve özel alanlar, ● Bölümler, birimler, ekipler ve çalışanlar, ● Çözüm ortakları, üçüncü taraflardan sağlanan servis, hizmet veya ürünler.
BGYS	Bilgi Güvenlik Yönetim Sistemi

5. BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKASI

5.1. Genel

- Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntıları, Tüm çalışanları ve üçüncü tarafları bilmek ve çalışmalarını bunlara uygun şekilde yürütmekle yükümlüdür.
- Bu kural ve politikaların, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.
- BGYS, TS ISO/IEC 27001 "Bilgi Teknolojisi (Information Technology) Güvenlik Teknikleri (Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri (Information Security Management Systems) Gereksinimler (Requirements)" standardını temel alarak yapılandırılmalı ve işletilmelidir.

- BGYS 'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmaları, ilgili tarafların katkısıyla yürütülmelidir.
- Kuruluş tarafından tüm çalışanlara veya üçüncü taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça kuruluşa ait sayılacaktır.
- Çalışanlar, tüm üçüncü parti şirketler (Kuruluş kaynaklarına iletişimi olan danışmanlar, firmalar vb.) ve Stajyerler ile gizlilik anlaşmaları yapılmalıdır.
- İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulamaya alınması esastır.
- Tüm Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut şirket çalışanlarına ve yeni işe başlayan çalışanlara verilmelidir.
- Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilmeli; ihlallere sebep olan uygunsuzluklar tespit edilmeli, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınması sağlanmalıdır.
- Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulmalı ve varlık sahiplikleri atanmalıdır.
- Kurumsal veriler sınıflandırılmalı ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenmelidir.
- Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulamaya konulmalıdır.
- Kuruluşumuza ait bilgi varlıkları kapsamında kuruluş içinde veya dışında maruz kalınabilecek fiziksel tehditlere karşı gerekli kontrol ve politikalar ayrıca geliştirilmeli ve uygulamaya alınmalıdır.
- Kapasite yönetimi, üçüncü taraflar ile ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilmeli ve uygulamaya alınmalıdır.
- Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ile ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanmalı; denetim kayıtlarının yetkisiz erişime karşı korunması sağlanmalıdır.
- Erişim hakları ihtiyaç nispetinde atanmalı; erişim kontrolü için mümkün olan en güvenli teknoloji ve tekniklerin kullanılması sağlanmalıdır.
- Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenip, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı düzenli aralıklarla kontrol edilmelidir.
- Kritik altyapı için süreklilik planları hazırlanmalı, altyapının bakımı ve tatbikatı yapılmalıdır.
- Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler ile sapmalar ve özel durumları işlemek için süreçler

tasarlanmalı, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanmalıdır.

5.2. Hedefler

- BGYS Politikası, Kuruluş çalışanlarına güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde Kuruluşun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflar ile yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla Kuruluşun tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedeflemelidir.

- Kuruluşumuzda belirlemiş olduğumuz iş stratejisi kapsamında; BGYS uygulama kültürünü hem iç hem dış paydaşlara entegre ederek; standardize edilmiş bir biçimde bilgi güvenliğini gizlilik, bütünlük ve erişilebilirlik kapsamında kesintisiz korumak ana hedeflerden olmalıdır.

- Yönetim Tarafından belirlenen hedefler belirli periyotlarda izlenmeli ve Yönetim Gözden Geçirme çalışmalarında gözden geçirilmelidir.

5.3. Bilgi Güvenliği Organizasyonu

- Kuruluş içi organizasyonumuzda; bilgi güvenliği rolleri ve sorumlulukları aşağıdaki başlıklar altında tanımlanır;
    - **Görevlerin Ayrılığı**; Çelişen görevler ve sorumluluklar, yetkilendirilmemiş veya kasıtsız değişiklik fırsatlarını veya kuruluş varlıklarının yanlış kullanımını azaltmak amacıyla ayrılma ilkesi ile belirlenmelidir.
    - Her bir varlık ya da bilgi güvenliği süreci için sorumluluk tahsis edilmeli ve sorumluluk detayları yazılı hale getirilmelidir.
    - Yetkilendirme seviyeleri belirlenmeli ve kayıt altına alınmalıdır.
    - Bilgi güvenliği sorumluluklarının tahsisi bilgi güvenliği politikaları ile uyumlu şekilde yapılmalıdır.
    - Varlıkların korunması ve özel güvenlik süreçlerinin yürütülmesi için yerel sorumluluklar açıkça tanımlanmalıdır.

5.4. Risk Yönetim Çerçevesi

- Kuruluşun risk yönetim çerçevesi; Varlıkların tanımlanması, Bilgi güvenliği risklerinin ve fırsatlarının belirlenmesi, değerlendirilmesini ve işlenmesini;
- Bilgi güvenliği risk yönetimi faaliyetleri ve artık risklerin kabulü için sorumlulukları ve;
- Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlamalıdır.
- Risk işleme planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme ve Yönetim Komitesi sorumlu sayılmalıdır.

- Tüm bu çalışmalar, ilgili prosedür ve talimatlar ile tanımlanarak kayıt altına alınmalıdır.
- Bilgi Güvenliğini tehdit eden unsurlar; iç tehdit ve dış tehdit unsurları olarak; bu politika ve diğer politikalar çerçevesinde ayrıntılı olarak ele alınmalıdır.

5.5. Politikanın İhlali ve Yaptırımlar

- BGYS Politikası ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için uygulanacak yaptırımlar tanımlanmalı ve çalışanlara da bildirilmelidir.
- Üçüncü taraflar için ise geçerli olan sözleşmelerde geçen ilgili maddelerde uygulanması muhtemel olan yaptırımlar belirlenmelidir.

5.6. Yönetimin Gözden Geçirmesi

- Yönetim gözden geçirme toplantıları BGYS Üst Yönetim Temsilcisi tarafından organize edilerek, yönetim ve bölüm yöneticileri katılımı ile gerçekleştirilmelidir.
- BGYS'nin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez organize edilmelidir.
- YGG Çalışmalarının şekli ve kuralları prosedürler ile kayıt altına alınmalıdır.

5.7. Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi

- BGYS Politikası'nın sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS ekibi sorumludur.
- Politika dokümanları; Kuruluşta ciddi bir değişiklik olmadığı sürece en az yılda bir kez gözden geçirilmelidir.
- Kuruluşun çevresinde, iş koşullarında, yasal şartlarda veya teknik ortamdaki değişimler ile sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da hemen gözden geçirilmeli ve bir değişiklik gerekiyorsa Yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır.
- Her revizyon hem iç hem de dış paydaşların erişebileceği şekilde yayınlanmalıdır.

6. DOKÜMAN TARİHÇESİ ve REVİZE TAKİP TABLOSU

Hazırlayan		***Gözden Geçiren***		***Yayına Sunan***
Yeşim ERKAN		Aydoğan OVAT	Ali Berkay BENGÜ	Yeşim ERKAN
Kalite ve Süreç		Bilgi Güvenliği ve Uyum Direktörü	BGYS Üst Yönetim Temsilcisi / EVP	Kalite ve Süreç
Rev. No	***Yayın/Rev. Tarihi***	***Yayın/Rev. Gerekçesi***		***Yayın/Rev. Sorumlusu***
00		İlk Yayın		Yeşim ERKAN