



BİLGİ GÜVENLİĞİ POLİTİKASI

17.05.2018

İÇİNDEKİLER

I. Tanımlar.....	2
II. Kapsam.....	2
III. Amaçlar	3
IV. Taahhütler	4
V. Onay ve Revizyonlar	5

I. Tanımlar

Bilgi Varlıkları: Kurum için değerli olan herhangi bir şeyi ifade eder (herhangi bir bilgi, yazılım, donanım, şahıs, Kuruma ait süreç).

Bilgi Güvenliği: Kuruma ait bilgilere sadece yetkili şahıslar tarafından erişilebilmesini ifade eder ve söz konusu bilgiler yetkili olmayan değişikliklere karşı korunur, bu tür değişiklikler onaylanır ve bilgi varlıkları ihtiyaç duyulduğunda erişilebilir olacaktır.

II. Kapsam

Bu politika Kurumun tüm çalışanlarını, üçüncü taraflar, bilgi sistemlerine destek sağlayan hizmet, yazılım ya da donanım sağlayıcılar olarak bilgi sistemlerine erişen kullanıcıları ve ziyaretçileri kapsar.

III. Amaçlar

Amaç, MAPFRE GROUP'un çalışanlarının MAPFRE GROUP'a ait kaynakları kullanırken uymaları gereken bilgi güvenliği kurallarının belirlenmesi suretiyle, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve Kurumun bilgilerini korumaktır.

IV. Taahhütler

- MAPFRE GROUP (Kurum) amaçları, değerleri ve stratejik hedeflerine uygun olarak bilgi güvenliğini vurgular.
- Kurumun yönetimi;
 - Kurumun güvenilirliğini ve imajını korumayı;
 - İmzalanmış olan sözleşmelerin bilgi güvenliği gerekliliklerini karşılamalarını sağlamayı; ve
 - Kurumun esas operasyonları ile destek operasyonlarının asgari kesinti ile devam etmesini sağlamayı hedefler.

Kurum, bu amaçlara yönelik olarak Kurumun bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve muhafaza etmek için önlemler almayı taahhüt eder.

- Bilgi güvenliği riskleri, Kurumun risk yönetimine uygun olarak tespit edilir, değerlendirilir ve işlenir. Risklerin yönetiminden Compliance ve Risk Yönetimi ile Bilgi Güvenliği Alanları sorumludur.
- Kurumun bilgi teknolojileri altyapısını kullanan ve bilgi kaynaklarına erişen herkesin
 - Şahsi ve elektronik iletişim ile üçüncü taraflarla bilgi alışverişi durumlarında Kuruma ait bilgilerin gizliliğini sağlamaları;
 - Risk seviyesine göre tespit edilen güvenlik önlemlerini almaları;
 - Bilgi güvenliği ihlalleri konusunda bilgi sahibi olmaları, bir ihlale yol açabilecek herhangi bir eylemden kaçınmaları ve Kurum tarafından belirlenen ve ilan edilen yöntemlerle gözlemlenen tüm bilgi güvenliği ihlali vakalarını rapor etmeleri;

- Yetkili olmayan şahıslarla dahili bilgi kaynaklarını paylaşmamaları ve dahili bilgi kaynaklarını Türkiye Cumhuriyeti'nin geçerliyasal düzenlemelerine aykırı eylemler için kullanmamaları gerekmektedir.
- Kurum çalışanlarının ve üçüncü şahıslar, tedarikçiler, müşteriler, misafirler vs. gibi harici tarafların, bu politikaya ve ayrıca bu politikanın uygulamaya konması için çıkarılan diğer politika, prosedür ve talimatlara uymaları gerekmektedir.
- Çevre ve Güvenlik Komitesi, bilgi güvenliği altyapısının işletimini desteklemekten ve muhafaza etmekten sorumludur.
- Kurum, tüm çalışanlarına e-egitim veya sınıf içi eğitim biçiminde "Bilgi Güvenliği Farkındalık Eğitimi" vermeyi, bilgi güvenliğini sürekli olarak geliştirmeyi ve geçerli mevzuat ile düzenlemelerle ilgili olarak tarafların uygulanabilir beklentilerini karşılamayı taahhüt eder.
- Bilgi güvenliği politikalarına, prosedürlerine ve talimatlarına uyulmadığı takdirde, Kurum personel düzenlemesi uyarınca uyarı, kınama, iş akdinin feshi vs. gibi çeşitli yaptırımlar uygular.
- Kurumun üst yönetimi, bilgi varlıklarının korunması, bilgi güvenliği farkındalığının yaratılması, ortak bir şirket kültürü geliştirilmesi, risklerin tespit edilmesi ve zayıf yönlerin ortadan kaldırılmasına yönelik gerekli önlemlerin alınması ve güvenlik ihlali durumlarında gerekli yaptırımların uygulanması için gerekli tüm desteği vermeye hazırdır.
- Kurum, iç ve dış denetimler, söz konusu denetimlerin sonuçlarının yönetime sunulması ve söz konusu sonuçlarla ilgili gerekli önlemlerin alınması aracılığıyla Bilgi Güvenliği ve Kişisel Verilerin Korunması Kanunu'nun gerekliliklerine uyulmasını sağlar. Ayrıca, uygulanabilir bilgi güvenliği kontrolleri ilgili taraflar ile birlikte belirlenir ve yönetilir.

V. Onay ve Revizyonlar

Bu Bilgi Güvenliği Politikası, İcra Kurulu tarafından 17.05.2018 tarihinde onaylanmıştır. Bu Politika, yılda en az bir kez Bilgi Güvenliği Yetkilisi tarafından gözden geçirilecek ve gerekli olduğu takdirde, İcra Kurulu tarafından tadil edilecektir. Ayrıca, içeriğini etkileyebilecek herhangi bir önemli değişikliğe uygun hale getirilmesi amacıyla bu Politika herhangi bir zamanda tadil edilebilir.