Continental
The Future in Motion

Bilgi Güvenliği kurumun bilgi varlıklarının gizlilik, bütünlük ve kullanabilirliğinin korunmasıdır

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,
Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,
Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

Kapsam

Bu politika, kurum Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

Hedef

Kurum yönetimi:

- Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak,
- Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
- Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak
- Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

Risk Yönetimi

Kurumun risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar.
Bu planın yönetiminden ve gerçekleştirilmesinden Bilgi Güvenliği Koordinasyon Ekibi sorumludur.

Görevler ve Sorumluluklar

Kurumun tüm çalışanları ve BGYS de tanımlanan dış taraflar, bu politikaya ve bu politikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür. Birimlerin güvenlik sorumlularından oluşan Güvenlik Koordinasyon Ekibi , BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.

Bilgi Güvenliği İlkeleri

Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:

- Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,
- Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
- Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi Güvenliği Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.
- Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
- Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel *Yönetmeliği* gereğince yaptırım uygulayabilir.

Bu politika, Güvenlik Koordinasyon ekibi tarafından periyodik olarak yılda bir gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Üst Yönetim tarafından onaylanır. Onaylanan politika ilgililere yayınlanır.

Kurum yönetimi olarak, "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederiz.