TAC A.Ş. Bilgi güvenliği ve siber güvenlik politikası bilginin, sadece yetkili kişiler tarafından erişilebilir olması, yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması, yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olmasını sağlamak üzere oluşturulmuştur.

Kurumumuz, destek ve hizmetlerinin bir kısmını elektronik ortamda gerçekleştirmektedir. Bu politika, kurum Bilgi İşlem alt yapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını, kapsamaktadır.

TAC A.Ş. yurt içi yurt dışı taahhüt uygulamaları yapmakta olup müşterilere ait bilgiler kurumun risk yönetim çerçevesi, bilgi güvenliği ve siber güvenlik risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği ve siber güvenlik risklerinin nasıl kontrol edildiğini tanımlar. Bu planın yönetiminden ve gerçekleştirilmesinden Bilgi Güvenlik ve Siber Güvenlik temsilcisi sorumludur.
TAC A.Ş. 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 ve siber güvenlik ihlal olaylarını raporlamalı ve Bilgi güvenliği ve Siber Güvenlik Birimine 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. Kurumun tüm çalışanları ve BGYS de tanımlanan dış taraflar, bu politikaya ve bu politikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür.
Birimlerin sorumlularından oluşan Bilgi Güvenlik ve Siber Güvenlik Kurulu, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur. Bilgi güvenliği ve siber güvenlik politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

1- **Uyarma,**
2- **Kınama,**
3- **Para cezası,**
4- **Sözleşme feshi**.

İş Sürekliliği ve Acil Durum Planları, Veri Yedekleme Prosedürleri, Virüs ve Saldırganlardan Korunma, Sistemlere Erişim Kontrolü, Bilgi Güvenliği ve Siber Güvenlik Olayları Prosedürleri bu politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır. Bu politika, Bilgi Güvenliği ve Siber Güvenlik Kurulu tarafından periyodik olarak her yıl gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği ve siber güvenlik uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika Kurum Başkanı tarafından onaylanır. Onaylanan politika kurum web sayfasında yayınlanır. Kurum yönetimi olarak, "Kurum Bilgi Güvenliği ve Siber Güvenlik Politikasının uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

GENEL MÜDÜR