

TÜMSAŞ	BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ	Yürürlük Tarihi: 05/06/2014
	BİLGİ GÜVENLİĞİ POLİTİKASI	Rev. T.:
		Rev. No: 0/00
		Sayfa No: 1 / 1

KURULUŞUMUZ BÜNYESİNDE BULUNAN BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİMİZİN SÜREKLİ GELİŞİMİNİ SAĞLAMAK İÇİN:

BİLGİ VARLIKLARINI TANIMLAMAYI BU VARLIKLARIN, İŞE ETKİSİNİ: varlığı yerine koyma maliyeti, bilginin gizliliği, imaja olan etkisi, yasal ve hukuki yükümlülükler bakımından yaratacağı zararı gibi konuları ele alarak,

TEHDİT OLASILIĞINI: zayıflıkların çokluğu ve varolan kontrollerin bu zayıflıkları ne kadar kapatabildiği, saldırgan motivasyonu, bilginin rakipler için cazibesi, erişim kontrollerindeki açıklar ve bilginin bütünlüğüne ilişkin tehlikeleri ele alarak,

BİLGİNİN GİZLİLİĞİ, BÜTÜNLÜĞÜ VE ERİŞİMİNE İLİŞKİN RİSKLERİ BELİRLEMİYİ, DEĞERLENDİRMEYİ, KABUL EDİLEBİLİR SEVİYENİN ÜZERİNDE BULUNAN TÜM VARLIKLAR İÇİN GEREKLİ KONTROLLERİ UYGULAMAYI, BİLGİ GÜVENLİĞİ SÜREÇLERİNİN PERFORMANSINI ÖLÇMEYİ, BU VERİLERDEN HEDEFLER ÜRETMEYİ, ZAYIFLIKLARIMIZI VE TEHDİTLERİ ALT YAPI, ÇALIŞMA ORTAMI, DONANIM, YAZILIM VE EĞİTİM YATIRIMLARIYLA EN AZA İNDİRGEMEYİ, İŞİMİZİN, MÜŞTERİLERİMİZİN VE YASAL ŞARTLARIN GEREKTİRDİĞİ GÜVENLİK ŞARTLARINI KARŞILAMAYI,

TAAHHÜT EDERİZ.

Politikalar, yönetimin gözden geçirme toplantılarında gözden geçirilmekte, belirlenen hedefler doğrultusunda gerektiğinde revize edilmektedir. Bilgi Güvenliğinde politikalar belirlenirken; bilginin işlenirken, iletilirken ve muhafaza edilirken Gizlilik, Bütünlük ve Erişilebilirlik esas alınacağı da anlatılmakta, risk yönetimi yaklaşımı da vurgulanmaktadır.

GENEL MÜDÜR

		