

KURULUŖUMUZ BÜNYESİNDE BULUNAN BİLGİ GÜVENLİĐİ YÖNETİM SİSTEMİMİZİN SÜREKLİ GELİŖİMİNİ SAĐLAMAK İÇİN:

BİLGİ VARLIKLARINI TANIMLAMAYI BU VARLIKLARIN, İŖE ETKİSİNİ: varlığı yerine koyma maliyeti, bilginin gizliliĐi, imaja olan etkisi, yasal ve hukuki yükümlölükler bakımından yaratacaĐı zararı gibi konuları ele alarak,

TEHDİT OLASILIĐINI: zayıflıkların çokluĐu ve varolan kontrollerin bu zayıflıkları ne kadar kapatabildiĐi, saldırgan motivasyonu, bilginin rakipler için cazibesi, eriŖim kontrollerindeki açıklar ve bilginin bütünlüĐüne iliŖkin tehlikeleri ele alarak,

BİLGİNİN GİZLİLİĐİ, BÜTÜNLÜĐÜ VE ERİŖİMİNE İLİŖKİN RİSKLERİ BELİRLEMİYİ, DEĐERLENDİRMEYİ, KABUL EDİLEBİLİR SEVİYENİN ÜZERİNDE BULUNAN TÜM VARLIKLAR İÇİN GEREKLİ KONTROLLERİ UYGULAMAYI, BİLGİ GÜVENLİĐİ SÜREÇLERİNİN PERFORMANSINI ÖLÇMEYİ, BU VERİLERDEN HEDEFLER ÜRETMEYİ, ZAYIFLIKLARIMIZI VE TEHDİTLERİ ALT YAPI, ÇALIŖMA ORTAMI, DONANIM, YAZILIM VE EĐİTİM YATIRIMLARIYLA EN AZA İNDİRGEMEYİ, İŖİMİZİN, MÜŖTERİLERİMİZİN VE YASAL ŖARTLARIN GEREKTİRDİĐİ GÜVENLİK ŖARTLARINI KARŖILAMAYI,

TAAHHÜT EDERİZ.

Politikalar, yönetimin gözden geçirme toplantılarında gözden geçirilmekte, belirlenen hedefler doğrultusunda gerektiĐe revize edilmektedir.

Bilgi GüvenliĐinde politikalar belirlenirken; bilginin iŖlenirken, iletilirken ve muhafaza edilirken Gizlilik, Bütünlük ve EriŖilebilirlik esas alınacaĐı da anlatılmakta, risk yönetimi yaklaŖımı da vurgulanmaktadır.

GENEL MÜDÜR