

ENTEĞRE YÖNETİM SİSTEMİ POLİTİKASI

KALİTE POLİTİKAMIZ:

TS EN ISO 9001:2015 Kalite Yönetim Sistemi, TS EN ISO 10002 Müşteri Şikâyetleri Yönetim Sistemi ve TS EN ISO 27001 Bilgi Güvenliği Yönetim Sistemin ana teması; "Bilgi Sistemleri Güvenliği altyapılarına ait donanım ve yazılım satışı, demo, kurulum, yerinde ve uzaktan teknik destek hizmetleri ile bu faaliyetlere ait danışmanlık, eğitim ve mühendislik hizmetleri."ne ait; insan, alt yapı, yazılım, donanım, kuruluş bilgileri, üçüncü şahıslara ait bilgiler ve finansal kaynaklar içerisinde bilgi güvenliği yönetiminin sağlandığını göstermek, risk yönetimini güvence altına almak, Kalite ve bilgi güvenliği yönetimi süreç performansını ölçmek ve bilgi güvenliği ile ilgili konularda üçüncü taraflarla olan ilişkilerin düzenlenmesini sağlamaktır.

Bu doğrultuda

Kalite ve Müşteri Memnuniyet Yönetim Sistemi Politikamız

- Kalite sistem sürekliliği ve iyileştirmeleri ile ilgili çalışmalarını planlayıp uygulayarak, kurumsal bir firma olma yolundaki çalışmaların sürekliliğini sağlamak, bunun için gerekli kaynak ve bütçe planlamasını yapmak,
- Uygulama geliştirme teknolojilerimizi ve araştırmalarımızı güncel tutmak, bünyesinde, yeni gelişen teknolojileri takip eden, yaptığı işin gerektirdiği eğitimleri almış yetenekli ve özgüveni yüksek personelin, KURULUŞ mensubu olmaktan onur duyarak çalıştığı bir kurum olmak,
- Mevzuat, yönetmelik ve şartnamelere uygun, müşteri isteklerini, kalite, güvenilirlik, maliyet ve zaman yönünden en iyi seviyede karşılayacak ürünler geliştirmek ve bu sayede müşteri memnuniyetini sürekli kılarak rekabet gücümüzü artırmak temel politikamızdır.

Bilgi Güvenliği Politikamız

- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak
- Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.
- Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.
- Risklerin işlenmesi için çalışma esaslarını ortaya koymak.
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek
- Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik Firmasal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak

- *Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini minimize edecek yetkinliğe sahip olmak*
- *Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.*
- *Firma itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.*