KOCAER ÇELİK A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

Kocaer Çelik San. ve Tic. A.Ş. uzun çelik sektörünün önde gelen Demir Çelik Ürünlerinin (Köşebentler, U ve C Şekilli Profiller, I ve H Şekilli Profiller, Düz ve Nervürlü Çubuklar, Tünel Profil ve Aksesuarları, Maden Profil ve Aksesuarları, Ray Profilleri, Kare çubuklar, Dikdörtgen Kesitli Lama ve Silmeler, Özel Kesitli Profiller) üreticilerindendir.

Misyonumuz, Toplumsal sorumluluk ve çevre bilinciyle paydaşlarımızı organizasyonumuzun bir parçası görerek, sürdürülebilir ürün ve hizmet kalitemiz ve yenilikçi yapımızla rekabet gücümüzü arttırmaktır.

Misyonumuz doğrultusunda;

• Tüm yasa, mevzuat ve sözleşme gerekliliklerini yerine getirmek, Bilgi Sistemleri Tebliği kapsamında tanımlanan bilgi güvenliği yükümlülüklerini eksiksiz olarak uygulamak,

• Yetkinlik, farkındalık ve motivasyon temelinde, çalışanların bilgi güvenliği bilincini artırmak ve düzenli eğitimlerle gelişimlerini sağlamak,

• Tüm bilgi sistemleri ve süreçlerine ait riskleri yılda en az bir kez değerlendirmek ve etkili risk yönetimi süreçleriyle kurumun itibarını ve bilgi varlıklarını korumak,

• Bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların ve görev tanımlarının belirlenmesini sağlamak; bilgi güvenliği hedeflerinin oluşturulması, bilgi sistemlerine ilişkin risklerin yönetimine dair süreçlerin tanımlanması ile bilgi güvenliği kontrollerinin tesis edilmesi, değerlendirilmesi ve gözetimini içeren kapsamlı bir bilgi güvenliği politikasını yürütmek,

• Bilgi güvenliği süreçlerinin etkin yürütülmesi amacıyla, bilgi sistemlerinden bağımsız, en az 5 yıl deneyimli ve teknik yeterliliğe sahip bir Bilgi Güvenliği Sorumlusu atanmasını sağlamak; bu kişinin doğrudan üst yönetime bağlı olarak görev yapmasını temin etmek,

• Kuruluşumuza ait tüm bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda korunmasını sağlamak,

• Kritik iş süreçlerine yönelik iş sürekliliği planları oluşturmak; bu planlarda kabul edilebilir kesinti süreleri ve veri kaybı sınırlarını tanımlamak ve test ederek işlerliğini sürdürmek,

• Güvenlik ihlallerini sistematik biçimde yönetmek; olay müdahale planları çerçevesinde tespit, kayıt, raporlama ve gerekli cezai yaptırımları devreye almak,

• Bilgi sistemlerine yönelik yılda en az bir defa yetkili ve bağımsız firmalarca sızma testlerinin gerçekleştirilmesini, test sonuçlarının analiz edilerek raporlanmasını ve tespit edilen bulgular doğrultusunda gerekli teknik ve idari önlemlerin alınmasını temin etmek,

• Yeni bilgi sistemleri ve kritik projelerin üst yönetim tarafından gözden geçirilmesini ve risk analizlerinin tamamlanmasını sağlamak,

• Bilgi güvenliği politikası ve ilgili tüm kontrollerin yılda en az bir kez gözden geçirilmesini, değerlendirilmesini ve gerekirse revize edilmesini sağlayan bir değerlendirme mekanizmasını uygulamak,

Bilgi Güvenliği Politikası, bilgi varlıklarının korunması amacıyla oluşturulmuş olup, üst yönetim tarafından onaylanarak yürürlüğe girmiştir. Söz konusu politika kapsamında; bilgi güvenliğine yönelik uygulamaların gerçekleştirilmesi, sistematik olarak yönetilmesi, sistemin sürekli iyileştirilmesi ve gerekli kaynakların sağlanması üst yönetim tarafından taahhüt edilmektedir.