KOCAER ÇELİK SANAYİ VE TİCARET ANONİM ŞİRKETİ BİLGİ GÜVENLİĞİ VE BİLGİ SİSTEMLERİ YÖNETİMİ POLİTİKASI

Kocaer Çelik olarak, bilgi güvenliğinin ve güvenilir bilgi sistemlerinin operasyonel sürekliliğimizin, kurumsal itibarımızın, müşteri ve paydaş güveninin ve sürdürülebilir büyümemizin temel unsurları olduğuna inanıyoruz.

Hedefimiz; bilgi varlıklarımızın gizliliğini, bütünlüğünü ve erişilebilirliğini korumak, bilgi sistemlerimizi güvenli ve mevzuata uygun biçimde yönetmek ve değişen tehditlere karşı kurumsal dayanıklılığımızı sürekli geliştirmektir.

Bu politika; şirket merkezimiz, tesislerimiz, şubelerimiz, iştiraklerimiz ve bağlı ortaklıklarımızdaki bilgi varlıklarını ve bilgi sistemlerini; çalışanlarımızı, yöneticilerimizi, stajyerlerimizi ve danışmanlarımızı, ayrıca sistemlerimize erişen veya bizim adımıza bilgi işleyen üçüncü tarafları kapsar.

Bu anlayış çerçevesinde;

- **Gizlilik, Bütünlük ve Erişilebilirlik:** Dijital ve fiziksel bilgi varlıklarımızı yetkisiz erişim, değişiklik, kayıp ve ifşaya karşı korumayı; iş ihtiyaçlarına uygun erişilebilirliği sağlamayı, işlediğimiz kişisel verileri, ticari sırlarımızı ve Ar-Ge verilerimiz dâhil fikri mülkiyetimizi korumayı,
- **Risk Temelli Yönetim:** Bilgi güvenliği risklerini yılda en az bir kez ve önemli sistem değişikliklerinde değerlendirmeyi; risk kabul ve işleme kararlarını üst yönetim onayıyla belirlemeyi, iyileştirme faaliyetlerini kaynak ve süreleriyle planlayarak izlemeyi,
- **Yönetişim ve Kaynak Tahsisi:** Yönetim Kurulumuzun gözetimi ve üst yönetimimizin liderliğinde sorumlulukları görevler ayrılığı ilkesine göre tanımlamayı; Bilgi Güvenliği Komitesi ve ilgili birimlerin eşgüdümünü sağlamayı, sorumlulukları yılda en az bir kez gözden geçirmeyi ve yeterli bütçe, insan kaynağı ve teknoloji tahsis etmeyi,
- **Bağımsız Gözetim ve Sorumluluk:** Mevzuatta aranan teknik yetkinliğe ve en az beş yıllık ilgili deneyime sahip bir Bilgi Güvenliği Sorumlusu belirlemeyi; bu rolün üst yönetime bağlı çalışmasını ve bilgi sistemlerinin yönetimine ilişkin uygulama görevleriyle çakışmamasını sağlamayı,
- **Bilgi Sistemleri Stratejisi ve Kritik Projeler:** Bilgi sistemleri stratejimizi şirketimizin hedefleriyle uyumlu geliştirmeyi; kritik sistem projelerini ve önemli değişiklikleri, risklerini değerlendirerek üst yönetim onayıyla hayata geçirmeyi,
- **Varlık Yönetimi ve Sınıflandırma:** Bilgi varlıklarımızın ve sistemlerimizin envanterini, sorumlularını ve kritik iş süreçleriyle bağımlılıklarını güncel tutmayı; bilgi varlıklarını gizlilik, bütünlük ve erişilebilirlik gereksinimlerini dikkate alarak kritiklik ve hassasiyetlerine göre sınıflandırarak her sınıflandırma seviyesi için uygun koruma önlemlerini, işleme ve saklama kontrollerini uygulamayı,

- **Denetim ve Teknik Doğrulama:** Bilgi sistemlerimizi ve güvenlik kontrollerimizi yılda en az bir kez iç denetim ve yetkili ve bağımsız kuruluşlarca gerçekleştirilen sızma testleriyle değerlendirmeyi; BGYS'mizi yılda en az bir kez ISO/IEC 27001 kapsamında akredite bir belgelendirme kuruluşunun dış denetimine tabi tutmayı; bulgular için üst yönetim onaylı iyileştirme planları oluşturmayı, gerekli teknik ve idari önlemleri uygulamayı ve sonuçlarını Yönetim Kurulumuza raporlamayı,
- **Kimlik ve Erişim Yönetimi:** Rol tabanlı erişim ve en az yetki ilkelerini uygulamayı; güçlü kimlik doğrulama yöntemlerini uygulamayı ve güvenli parola standartları oluşturmayı; kritik sistemlerde ve ayrıcalıklı hesaplarda çok faktörlü kimlik doğrulamayı kullanmayı; yetkileri yılda en az bir kez ve görev değişikliği veya işten ayrılma durumunda gözden geçirerek gereksiz erişimleri kaldırmayı,
- **Ağ ve Sistem Güvenliği:** Katmanlı güvenlik yaklaşımıyla ağlarımızı, sistemlerimizi ve cihazlarımızı korumayı; fabrika ortamındaki endüstriyel kontrol ve MES sistemlerini ofis ağlarından mantıksal olarak ayrıştırmayı ve erişimleri işin gerektirdiği kapsamla sınırlandırmayı,
- **Fiziksel ve Çevresel Güvenlik:** Bilgi işlem merkezlerimizin ve sistem odalarımızın fiziksel ve çevresel güvenliğini sağlamayı; erişim kontrolü, yangın algılama ve söndürme, kesintisiz güç kaynağı, iklimlendirme ve ortam izleme önlemlerini tesis ederek etkinliklerini ve sürekliliklerini düzenli olarak denetlemeyi,
- **Olay Yönetimi ve Zamanında Bildirim:** Güvenlik olaylarına ve zafiyetlere yönelik müdahale planlarını oluşturmayı; çalışanlarımızın ve ilgili üçüncü tarafların şüpheli durumları tanımlı kanallardan derhal bildirmelerini sağlamayı; bilgi güvenliği ihlallerinin ve ihlal şüphelerinin Etik Hat üzerinden de bildirilebilmesini sağlamayı; olayları kayıt altına alıp yılda en az bir kez değerlendirmeyi, nedenlerini gidererek tekrarını önlemeyi ve uygulanabilir yasal bildirim yükümlülüklerini yerine getirmeyi,
- **Tedarikçi ve Dış Hizmet Güvenliği:** Bulut hizmetleri dâhil dışarıdan sağlanan bilgi sistemleri hizmetlerinin risklerini ve güvenlik uyumunu gözetmeyi; sözleşmelerde gizlilik, hizmet sürekliliği, veri koruma, hizmetin sonlandırılması ve uygulanabilir denetim erişimi şartlarını güvence altına almayı; tedarikçi ve dış hizmet sağlayıcıların bilgi güvenliği yükümlülüklerine uyumlarını ve performanslarını periyodik olarak denetlemeyi,
- **İş Sürekliliği ve Kurtarma:** Kritik bilgi sistemleri için kabul edilebilir kesinti ve veri kaybı hedeflerini belirlemeyi; süreklilik, yedekleme ve kurtarma planlarını hazırlamayı, yılda en az bir kez test ederek güncellemeyi ve kesintilerde öncelikli faaliyetlerin zamanında yeniden yürütülmesini sağlamayı,
- **Eğitim ve Güvenlik Kültürü:** Çalışanlarımıza rol ve sorumluluklarına uygun bilgi güvenliği eğitimlerini yılda en az bir kez vermeyi; Ar-Ge, kişisel veri ve ticari sırlarla çalışan birimlerde farkındalığı güçlendirmeyi ve güvenli çalışma alışkanlıklarını kurum kültürümüze yerleştirmeyi,

- **Kayıt ve Denetim İzleri:** Kritik işlem ve erişim kayıtlarını oluşturmayı, bütünlüklerini ve güvenliklerini korumayı, uygulanabilir saklama süreleri boyunca muhafaza etmeyi ve olağandışı faaliyetleri düzenli izleyerek gerekli önlemleri almayı,
- **Mevzuata Uyum ve Sorumlu Davranış:** Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimi Tebliği, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve şirketimize uygulanabilir diğer düzenlemelere ve sözleşmesel yükümlülüklerimize uymayı; ihlalleri mevzuat, iç düzenlemeler ve sözleşmeler çerçevesinde değerlendirmeyi ve gerektiğinde ilgili disiplin, hukuki ve sözleşmesel yaptırımların uygulanmasını sağlamayı,
- **BGYS'nin Etkinliği ve Sürekli İyileştirme:** ISO/IEC 27001 çerçevesinde Bilgi Güvenliği Yönetim Sistemimizin gerekliliklerini karşılamayı ve etkinliğini sürekli iyileştirmeyi; ölçülebilir hedefler belirlemeyi, kontrol sonuçlarını izlemeyi ve iyileştirme faaliyetlerini takip etmeyi,

taahhüt ederiz.

Bu politikanın Yönetim Kurulumuzun onayı, üst yönetimimizin gözetimi, tüm çalışanlarımızın katılımı ve ilgili tarafların sorumluluklarını yerine getirmesiyle hayata geçirilmesini esas alıyoruz. Politikamızı yılda en az bir kez gözden geçirerek iş ihtiyaçları, tehditler ve mevzuat değişiklikleri doğrultusunda güncelliyor, çalışanlarımıza ve ilgili taraflara duyuruyoruz.