Çolakoğlu Metalurji

BİLGİ GÜVENLİĞİ POLİTİKASI

Çolakoğlu Metalurji A.Ş., bilgi güvenliğinin gerçekleştirilmesi, işletimi, sürekli izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gereken her türlü adımın atılacağını taahhüt eder. Bilgi güvenliği, tüm çalışanların sorumluluğu olup kurumsal kültürün ayrılmaz bir parçasıdır.
Bilgi güvenliği, bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasıyla mümkündür:

- Gizlilik: Bilgiye yalnızca yetkili kişilerin erişmesi,
- Bütünlük: Bilginin doğruluğunun ve tamlığının korunması, yetkisiz değişimlerden korunması,
- Erişilebilirlik**:** Bilginin ihtiyaç duyulduğunda yetkili kişilerce kullanılabilir olmasıdır.

Çolakoğlu Metalurji A.Ş., bilgi güvenliği hedeflerini belirleyerek, bu hedeflere yönelik uyumluluğu düzenli olarak izler ve ölçer; yönetim sistemini risk bazlı düşünme yaklaşımı doğrultusunda uygular, yürütür ve sürekli iyileştirir. Operasyonel Teknolojiler (OT) kapsamında gerekli bilgi güvenliği kontrollerini gerçekleştirerek ilgili standartlara uyumu sağlar ve enerji üretimi faaliyetlerine ilişkin yürürlükteki yasal düzenlemeler ile standartlara uymayı taahhüt eder. Yasal, mevzuat ve sözleşme gerekliliklere tam uyum sağlar; sunduğu ürün ve hizmetlerin müşteri ve paydaş beklentilerini karşılamasını ve müşteri bilgilerinin korunmasını güvence altına alır. İç ve dış paydaşlarının ihtiyaç ve beklentilerini dikkate alarak, iş süreçlerinin güvenliği ile üretim sürekliliğinin korunmasını hedefler.

Çolakoğlu Metalurji, yukarıda belirtilen ilkelere bağlı kalarak, bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlar doğrultusunda gerçekleştirmeyi hedefler;

- Bilgi Güvenliği Yönetim Sistemi (“BGYS”) ile, uluslararası olarak kabul edilmiş standartlar doğrultusunda planlanır, gerçekleştirilir ve geliştirilir.
- BGYS hedefleri, politika çerçevesinde periyodik olarak belirlenir. Sistemin etkinliği, hedeflere ulaşma düzeyi ve risk durumu, üst yönetime periyodik olarak raporlanır. Yönetim, raporlar doğrultusunda stratejik kararlar alır ve gerekli kaynakları tahsis eder.
- BGYS’nin sürekli iyileştirilmesi için gerekli iç denetim, yönetimin gözden geçirmesi, düzeltici faaliyetler ile risklerin ve fırsatların belirlenmesi için atılması gerekli adımlar, yönetim ve yönetimin bilgi güvenliği sorumluluğunu verdiği ekipler tarafından sağlanır. Bilgi güvenliği ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır.
- BGYS çerçevesinde gerekli çalışmaların gerçekleştirilmesi için kaynaklar ve yönlendirmeler yönetim tarafından sağlanır.
- Tüm çalışanların yetkinliklerinin ve yönetim sistemlerine bağlılıklarının sürdürülmesi amacıyla, düzenli eğitimler ve farkındalık çalışmaları yürütülür. Açık ve şeffaf bir iletişim ortamı oluşturularak, çalışanların bilgi ve deneyimleri doğrultusunda sistemin sürekli iyileştirilmesine katılımı sağlanır.
- Kurumumuzun enerji üretim tesislerinde kullanılan operasyonel teknoloji (OT) ve endüstriyel kontrol sistemlerinin dahil tüm bilgi güvenliği risklerini yönetmek için risklerini değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilir ve olası riskleri önlemek için çalışmalar gerçekleştirilir.
- Paydaşları ile birlikte kurumun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir.

- BGYS kapsamında, bilgi varlıkları belirlenir, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliği beklentileri değerlendirilir, yasal ve sözleşmelere bağlı yükümlülükler değerlendirilir.
- Kurum, BGYS ile ilgili tüm yasal, mevzuat ve sözleşme gerekliliklere uymayı taahhüt eder. Tüm sözleşmelerde bilgi güvenliği gereksinimleri, gizlilik hükümleri, veri koruma ve ihlal bildirim yükümlülükleri açıkça tanımlanır. Üçüncü taraflarla yapılan anlaşmalarda bilgi güvenliği kontrollerinin entegrasyonu sağlanır.
- Bilgi güvenliği ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, yaşanması durumunda koordineli şekilde yanıt verilir.
- Kurum, bilgi güvenliği ihlallerine karşı Siber Olay Müdahale Ekibi (SOME) planlarını oluşturur, uygular ve test eder.
- Tüm bilgi sistemleri, cihazlar ve ağ bileşenleri; yetkisiz erişimi, yetki aşımını ve güvenlik açıklarını en aza indirmek amacıyla kurum tarafından belirlenen güvenlik standartları ve en iyi uygulamalar doğrultusunda güvenli bir şekilde yapılandırılır ve yönetilir. Kritik güvenlik yamaları ve güncellemeler düzenli olarak uygulanır.
- BGYS kapsamında riskleri yönetmek için, risk değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler ve olası riskleri önlemek için çalışmalar gerçekleştirilir.
- Müşteri ve paydaşlarının kişisel verileri dahil tüm bilgilerinin yetkisiz kişilerin eline geçmesi engellenir. Kişisel Verilerin Korunması Kanunu dahil ilgili kanun ve yönetmeliklerle uyumlu hale gelmesi için gereken çalışmalar yapılır.
- Yeni teknolojilerin devreye alınması öncesinde, bilgi güvenliği açısından güvenlik değerlendirmeleri gerçekleştirilir.
- BGYS'yi etkin biçimde yöneterek bilgi güvenliği kaynaklı yaşanabilecek zararlar asgariye indirilir.
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediği durumda hedeflenen kurtarma süresi içerisinde çalışabilir hale gelmesi sağlanır.
- BGYS kapsamında müşterilerimizin bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği sağlanır.
- BGYS içerisinde ele alınan değişiklik süreçlerinin yaşam döngüsü içerisinde işletilmesi sağlanır.
- Yönetim sistemlerinin amaçlanan sonuçları yerine getirme başarısı periyodik olarak gözden geçirilir, gerekli iyileştirmelerin zamanında hayata geçirilmesi güvence altına alınır.
- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerinin güvenliğinin sağlanmasına önem vermekte, iş süreçleri ile entegre, uyumlu ve dengeli olması hedeflenir.
- Entegre ve dinamik iş stratejisi bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılar.
- Güvenli çalışma alanları, arşiv odaları, sistem odaları gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemlerin alınması sağlanır.
- Tedarikçi ilişkilerinin güvenli bir şekilde yürütülmesi amacıyla; tedarik hizmetlerinin gözden geçirilmesi, meydana gelen değişikliklerin yönetilmesi için politikalar oluşturulur, özellikle bilgi teknolojileri tedarikçileri ile yapılan/yapılacak olan ve bilgi güvenliği risklerinin ifade edildiği anlaşmalarda güvenlik gereksinimleri belirlenir.

11/12/2025

Uğur DALBELER

Genel Müdür