Çolakoğlu Metalurji

BİLGİ GÜVENLİĞİ POLİTİKASI

Çolakoğlu® Metalurji A.Ş. bilgi güvenliğinin gerçekleştirilmesi, işletimi, izlenmesi, gözden geçirilmesi, bakımı ve iyileştirilmesi için gereken her türlü adımın atılacağını taahhüt eder. Çolakoğlu® Metalurji, bilgi güvenliği yönetimi ile ilgili olarak kapsam dahilindeki süreçlerde aşağıdaki ilkeleri benimsemektedir:

- Müşterilerine ve paydaşlarına sunduğu ürün ve hizmetlere ilişkin faaliyetlerin güvenliğinin sağlanmasına önem vermektedir.
- İş süreçleri ile entegre, uyumlu ve dengeli olması hedeflenmektedir. Entegre ve dinamik iş stratejisi, bilgi varlıklarının güvenliğini ve sürekliliğini gerekli kılmaktadır.
- Müşteri ve paydaşlarına değer sağlayan ürün ve hizmetlerin gizlilik, bütünlük ve erişilebilirliğini tehdit edebilecek risklere karşı tedbir almayı ilke edinir.
- Bu politika ve organizasyonun amacı ile uyumlu bilgi güvenliği hedefleri belirlenir ve düzenli aralıklarla uyumluluk ölçülerek, sürekli iyileştirme fırsatları değerlendirilir.

Bilgi güvenliği, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ile mümkündür.

Bilginin;

- Gizlilik gerekliliği, sadece yetkili kişiler tarafından erişilebilir olmasını,
- Bütünlük gerekliliği, bilgi varlıklarının tam ve doğruluğunun sağlanmasını, yetkisiz değişimlerden korunmasını,
- Erişilebilirlik gerekliliği, bilgi varlıklarının ihtiyaç duyulduğu anda yetkili kullanıcılar tarafından kullanılabilir olmasını ifade eder.

Çolakoğlu® Metalurji, yukarıda belirtilen ilkelerden taviz vermeden bilgi güvenliği çalışmalarını aşağıda belirtilen amaçlarla gerçekleştirmeyi hedefler:

- Bilgi Güvenliği Yönetim Sistemi (BGYS), uluslararası alanda kabul edilmiş [ISO7IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi] standardı şartları doğrultusunda planlanır, gerçekleştirilir ve geliştirilir.
- Kişisel Verilerin Korunması Kanunu dahil, ilgili kanun ve yönetmeliklerle uyumlu hale gelmesi için gereken çalışmaları yapar. 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 sorumluluğu verdiği ekipler tarafından sağlanır. Bilgi güvenliği ile ilgili tüm rol ve sorumluluklar belirlenir ve yönetim tarafından yetkilendirmeler yapılır.
- Bilgi Güvenliği Yönetim Sistemi çerçevesinde, gerekli çalışmaların gerçekleştirilmesi için kaynaklar yönetim tarafından sağlanır.
- Paydaşları ile birlikte kuruluşun rekabet avantajını olumsuz yönde etkileyebilecek maddi ve manevi kayıplar engellenir.
- Bilgi Güvenliği Yönetim Sistemi kapsamı; bilgi varlıkları belirlenerek, müşteriler, tedarikçiler ve iş ortakları gibi ilgili tarafların bilgi güvenliği beklentileri değerlendirilerek, varsa yasal ve sözleşmeli yükümlülükler değerlendirilerek yönetim tarafından iş stratejileri doğrultusunda belirlenir.
- Bilgi güvenliği risklerini yönetmek için riskleri değerlendirme, risk analizi ve risk işleme çalışmaları gerçekleştirilerek, gerekli tedbirler geliştirilir ve olası riskleri önlemek için çalışmalar gerçekleştirilir.
- Müşteri ve paydaşlarının kişisel verileri dahil, tüm bilgilerinin yetkisiz kişilerin eline geçmesi engellenir.
- Son kullanıcı bilgi güvenliği farkındalığı ve bu farkındalığın sürekli arttırılması sağlanır.

Çolakoğlu Metalurji

- Bilgi güvenliğini etkin biçimde yöneterek, bilgi güvenliği kaynaklı yaşanabilecek zararlar asgariye indirilir.

- Bilgi güvenliği ihlal olayı yaşama ihtimalini düşürmek için gerekli çalışmalar yapılır, gerçekleşmesi durumunda koordineli şekilde yanıt verilir.
- Kritik iş süreçlerinde yaşanabilecek kesintilerin önüne geçilmesi için gerekli düzenlemeler yapılır, geçilemediği durumda hedeflenen kurtarma süresi içerisinde tekrar çalışabilir hale getirilir.
- Bilgi Güvenliği Yönetim Sistemi kapsamında müşterilerimizin bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği sağlanır. Müşteri ile ilgili kritik iş süreçleri devamlı hale getirilir.
- Bilgi Güvenliği Yönetim Sistemi sürekli iyileştirilir.
- Güvenli çalışma alanları, arşiv odaları, sistem odaları gibi kurum içi çalışma bölgelerinde ve kurum çevresinde güvenliğin sağlanması için gerekli önlemler alınır.
- 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.

29/11/2018

Uğur DALBELER

Genel Müdür