

KOÇ METALURJİ A.Ş. (“ŞİRKET”) BİLGİ GÜVENLİĞİ POLİTİKASI

1. Kapsam

Koç Metalurji A.Ş.’nin stratejik planlarının desteklenmesi, sahip olunan marka değerinin korunması ve ilgili yasal düzenlemelere uyum sağlanması amacıyla izlenmesi gereken bilgi güvenliği kuralları ve prensipleri ile bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanması bu Politika kapsamındadır. Şirket mülkiyetinde olan her türlü bilgi ve bilgi varlığı bu Politika kapsamında olup, Şirket bünyesinde yerine getirilen tüm faaliyetler ve işletilen süreçler bu Politikaya uygun olarak yürütülür.

2. Amaç

Şirket bilgi varlıklarının siber saldırılardan korunmasına yönelik politika, prosedür, organizasyon vb. güvenlik kontrollerini sağlamak için “Bilgi Güvenliği Yönetimi Sistemi” tasarlanmıştır. Bunun anlamı; bilgilerin yetkili ellerde kalması, bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması ve bilgilerin, sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır.

Bilgi Güvenlik Yönetim Sistemi; güvenlik stratejisinin belirlenmesi, güvenlik politikalarının oluşturulması ve uygulanması, güvenlik sistemlerinin kurulumu, yönetimi ve izlenmesi süreç ve operasyonlarını içerir.

Bilgi Güvenliği Politikası, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII-128.9 Bilgi Sistemleri Yönetimi Tebliği (Tebliğ) ve konuyla ilgili Kişisel Verilerin Korunması Kanunu dikkate alınarak hazırlanmıştır.

Şirket, Bilgi Güvenliği ile ilgili aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

- 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 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 kurumsal 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,
- Kurum itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak,
- Bilgi Güvenliği Yönetim Sisteminin sürekliliğini sağlamak,
- Bilgi Güvenliği Yönetim Sistemini sürekli iyileştirmek amacıyla tüm çalışmalara destek vermek.

3. Roller ve Sorumlular

a. Yönetim Kurulu:

Bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve Yönetim Kurulu tarafından onaylanır. Bilgi güvenliği politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi Yönetim Kurulunun sorumluluğundadır. Yönetim Kurulu, politikanın gözetiminden sorumlu “Üst Yönetim” i yetkilendirir. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

b. Üst Yönetim:

Üst Yönetim, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından, sürekliliğinin sağlanmasından, bu politikanın, güncel olarak yaşamasını ve Şirket ve iştiraklerinin işle ilgili gerekliliklerini veya bilgilerinin ve bilgi sistemlerinin karşı karşıya olduğu risk ortamındaki ya da tehditlerdeki değişimleri yansıtmaya devam etmesini temin edecek şekilde devamlı gözden geçirilmesinden sorumlu olacaktır. Politika kapsamında hazırlanması gereken tüm standart, prosedür ve talimatların onaylanması için Yönetim Kurulu tarafından, ***Finans ve Mali İşler Direktörlüğü’nden oluşan Üst Yönetim yetkilendirilmiştir***

Bilgi güvenliği politikasının uygulanması Üst Yönetim tarafından gözetilir. Üst Yönetim, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlar ve gerekli yönetsel sorumlulukları tanımlar.

Üst Yönetim’in gözetimi ve sorumluluğu aşağıdaki gibidir:

- Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,
- Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,
- Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,
- Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi.
- Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürler, organizasyonel ve yönetsel yapı içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve takipler gerçekleştirilir.

- Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir **Bilgi Sistemleri Güvenliği Sorumlusu** belirlenir.
- Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir.

c. Bilgi Sistemleri Güvenliği Sorumlusu

Bilgi Sistemleri Güvenliği Sorumlusu, bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olup, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip kişidir. Genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik eder, politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlar. Ayrıca bu politika gereklerinin tüm çalışanlara (daimî veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır. Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği Bilgi Sistemleri Güvenliği Sorumlusu tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Şirket bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

Bilgi Güvenliği Yöneticisinin sorumlulukları aşağıdaki gibidir:

- Bilgi güvenliği farkındalık eğitimlerinin etkinliğini ölçmek ve sonuçlarını değerlendirmek.,
- Şirket Bilgi Güvenliği Politikası, Standartları ve Prosedürlerini gözden geçirmek ve gerekli değişiklikler için önerilerde bulunmak,
- Güvenlik zaafı ve olaylarının nedenlerini araştırmak; gerektiği zamanlarda delilleri saklamak ve raporlar, önlemler ve iyileştirme önerilerinde bulunmaktan sorumludur.
- Belirlenen kritik kontrollerin uygulanmasını sağlamak,
- İş sürekliliği planının işletilmesi, denetlenmesi ve testlerinin yapıldığını kontrol etmek,
- İlgili otorite ve çalışma grupları ile iletişim ve koordinasyonun sağlamak,
- Dış taraflara karşı kurumu temsil etmek ve ilgili faaliyetlerde koordinasyonu sağlamak,
- Bilgi sistemleri güvenliğiyle ilgili risklerle bu risklerin yönetimi hususunda üst yönetime rapor sunmak.

d. Kurum Personelinin Sorumlulukları:

Bilgi Güvenliği Yönetim Sistemi kategorisinde yayınlanmış tüm politika ve prosedürlere uymakla, gerçekleşmiş ya da olası güvenlik ihlallerini ve zafiyetlerini bildirmek ve Şirket tarafından talep edilen tüm faaliyetleri gerçekleştirmekle yükümlüdür.

Şirket çalışanları konumları veya görevleri ne olursa olsun işlerini, bilgilerin Şirket bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur. Bilgi Güvenliği Politikaları ister tam zamanlı ister yarı zamanlı, daimî ya da sözleşmeli olsun, tüm bilgileri veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur.

Bu bağlamda Varlık ve Süreç Sahipleri;

- Kendilerine duyurulan Bilgi Güvenliği Politikasına ve prosedürlerine uymak,
- Kendi süreç ve sistemlerinin yönetimleri için oluşturacakları süreç, akış, talimat, kılavuz, form gibi dokümanlarda Bilgi Güvenliği dokümanlarına uyumu sağlamak,
- Bilgi Güvenliği politikalarına ve/veya prosedürlerine uyumun sağlanmadığı veya bilgi güvenliği ihlal olaylarında yatirimciiliskileri@kocmetalurji.com.tr adresine bildirmek,
- Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak,
- Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Sistemleri Güvenliği Sorumlusuna bildirmek,
- Bilgi ve kurumsal kaynaklarına iş ihtiyaçları ölçüsünde erişim talebinde bulunmak,
- Sahibi olunan varlığın ve Kişisel Verilerin, erişim haklarını ve kimlerin yönetici ve kullanıcı bazında hangi ayrıcalıkla erişilebileceğini tayin etmek,
- Varlık envanterini gözlemek ve güncelliğini sağlamak,

Bilgi Güvenliği Politikası ilkeleri, Şirket İnsan Kaynaklarının Personel Yönetmeliği Kurallarına paralel uygulanmaktadır. Şirket çalışanı “Bilgi Güvenliği Politikasının” farkında olmaktan ve bu ilkelere uymaktan sorumludur.

Herhangi bir Şirket çalışanı Bilgi Güvenliği Politikaların gelişmesi ve Şirket’ in ihtiyaç duyduğu kontrolleri daha iyi yansıtmayı amacıyla politikaların değiştirilmesi konusunda **Bilgi Sistemleri Güvenliği Sorumlusu**’ na talepte bulunabilir. Yapılan talepler **Bilgi Sistemleri Güvenliği Sorumlusu** tarafından ele alınır ve değerlendirilir.

Üçüncü Taraflar:

Şirket’e mal ve hizmet sağlayan üçüncü kişilerin ve bunların çalışanlarının uyması gereken bilgi güvenliğine ilişkin düzenlemeler, ilgili sözleşmeler ve güvenlik protokolleri ile belirlenir.

Bunlar asgari aşağıdaki hususları kapsar:

- Sözleşmeler veya protokoller ile bildirilen bilgi güvenliği kuralları başta olmak üzere üçüncü taraflarla ilişkileri düzenleyen Şirket Politika ve Prosedürleri’ ne uygun hareket etmek.
- Şirket’e ait bilgi ve varlıkları Şirket onayı ve izni olmadan başkaları ile paylaşmamak,
- Şirket tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak,
- Şirket’in onay ve izni olmadan, Şirket’in cihazlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydını almamak, resmini, videosunu çekmemek, veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.
- Şirket lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

Şirket personeli sınıflandırmasına girmeyen ve Şirket bilgilerine erişim gereği olan üçüncü şahıs hizmet sağlayıcıları ve bunların bağlı destek personeli gibi tüm kişilerin, bu politikanın genel ilkelerine ve uymak zorunda oldukları diğer güvenlik sorumluluklarına ve yükümlülüklerine bağlı kalması şarttır.

4. Denetim ve Kontrol

Şirket bilgi sistemlerine ilişkin riskleri belirlemek, ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreç ve prosedürlerini tesis eder ve güncelliğini sağlar. Bilgi sistemlerine ilişkin risk analizi, risk işleme ve gözetim süreçleri işletilir. Risk analizi yılda en az bir defa gerçekleştirilir. Bilgi sistemlerinde meydana gelecek önemli değişikliklerde tekrarlanır. Risk analizinde tüm bilgi varlıkları değerlendirmeye alınır.

Bilgi sistemleri süreçleri ve kontrollerine ilişkin etkinlik, yeterlilik ve uyumluluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilir ve değerlendirilir. Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri ve yapılan çalışmalar yılda en az bir kez üst yönetime raporlanır ve gerekli önlemlerin alınması sağlanır.

Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği a. Bilgi Sistemleri Güvenliği Sorumlusu tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Şirket bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

Her birim yöneticisi Bilgi Güvenliği Politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derecede sorumludur.

Bilgi Güvenliği Politikası ihlalleri, Şirket'in risklere karşı ihtiyaç duyulan kontrollerin uygulanmaması neticesinde zarar görmesine, ayrıca yeni Türk Ceza Kanuna göre de cezai sorumluluk doğurmasına ve maddi zararların tazmini sorumluluğuna sebep olabilecektir. Dolayısıyla söz konusu ihlal aynı zamanda Şirket Personel Yönetmeliği ihlali olup disiplin cezası sonucunu doğurabilir. Gerek gözetim gerek denetim gerekse ihbar sonucu tespit edilen Bilgi Güvenliği Politikası ihlalleri şirket içi disiplin cezalarının uygulanması, istihdama son verilmesi hatta Adli ve Cezai yasal işlemler başlatılması ile sonuçlanabilecektir.

5. Hedefler

Şirket Bilgi Güvenliği, Şirket'in itibarının, güvenilirliğinin, bilgi varlıklarının korunması, temel ve destekleyici iş faaliyetlerinin mümkün olan en az kesinti ile devam etmesi amacıyla,

- Bilgi sistemlerinin sürekliliğini tam olarak sağlamayı,
- Çalışanların farkındalık ve güvenlik gereksinimlerine uyum düzeylerini en üst seviyeye çıkarmayı,
- Üçüncü taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,
- Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi,
- Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve saklanmasını,

6. Yürürlük

İşbu Bilgi Güvenliği Politikası **27/06/2025** tarihli Yönetim Kurulu kararı ile onaylanarak, yürürlüğe girmiştir. Bilgi Güvenliği Politikasında herhangi bir değişiklik gerektiğinde, değişiklik yapılan hususlar Yönetim Kurulu onayından geçtikten sonra geçerlilik kazanır. Onaylanan Bilgi Güvenliği Politikası tüm çalışanlarına ve konu ile ilgili olanlara duyurulur.

7. Yürütme

Bu Politika hükümleri Genel Müdürlük makamı tarafından yürütülür.