1. Bilgi Güvenliği Politikası Amacı, Kapsamı

Bilgi Güvenliği Politikasının amacı, Arçelik bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğinin sağlanması amacıyla gerekli gereksinimlerini tanımlamaktır.

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 diğer düzenlemeler dikkate alınarak hazırlanmıştır.

Arçelik özellikle aşağıda belirtilen konuların yerine getirilmesini benimsemiştir:

- Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetilmesini,
- Bilgi Güvenliği Standartlarının gerekliliklerini yerine getirmeyi,
- Bilgi Güvenliği ile ilgili tüm yasal mevzuata uyum sağlamayı,
- Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için gerekli kaynakları sağlamayı, kontrolleri tesis etmeyi, sürekli iyileştirme fırsatlarını değerlendirmeyi ve gözetim için gerekli çalışmaları gerçekleştirmeyi,
- Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmeyi,

Arçelik, Bilgi Güvenliği Yönetim Sistemi süreçlerinin işletilmesi ve sürekliliğinin sağlanması için gereken kontrollerin tesis edilmesini ve gözetimini bu politikaya bağlı alt politikalar, prosedürler ve talimatlar vasıtasıyla sağlar.

Bilgi Güvenliği Politikaları, ister tam zamanlı, ister yarı zamanlı, daimi ya da sözleşmeli olsun, tüm bilgileri veya iş sistemlerini kullanan tüm personel için, coğrafi konumdan veya iş biriminden bağımsız olarak geçerli ve zorunludur. Bu sınıflandırmalara girmeyen ve Arçelik 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.

2. Sorumlular

Yönetim Kurulu ve Üst Yönetim:

Yönetim Kurulu etkili bir bilgi güvenliği yönetim yapısının tesis edilmesi amacıyla, bilgi güvenliği stratejisi ve yol haritasının belirlendiği Bilgi Güvenliği Politikasını onaylar ve uygulanmasını zorunlu tutar. Politika kapsamında hazırlanması gereken tüm standart, prosedür ve talimatların onaylanması için Yönetim Kurulu tarafından, Strateji & Dijital GMY, Finansman & Mali İşler GMY, Hukuk ve Uyum Direktörü'nden oluşan Üst Yönetim yetkilendirilmiştir. Üst Yönetim, Bilgi Güvenliği Yönetim Sistemi'nin kurulması ve işletilmesi için gerekli kaynak ve yetki / sorumluluk tahsislerini gerçekleştirir Üst Yönetim, Yönetim Kurulunu temsilen, periyodik olarak bilgi güvenliği sisteminin gözden geçirmelerinin yapıldığı Bilgi Güvenliği Komitesine katılım sağlar. Üst yönetim, "Bilgi Güvenliği ve Siber Güvenlik Yönetimi" sorumlusu Yönetim Kurulu üyesine raporlar.

Tüm Çalışanlar:

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

Bilgi Güvenliği'nin ve bu politikanın amacı, bilgilerin ve tüm destek iş sistemlerinin, süreçlerinin ve uygulamalarının gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak, sürdürmek ve yönetmektir. Bunun anlamı; bilgilerin yetkili ellerde kalması; bilgilerin eksiksiz, doğru ve kullanılabilir durumda olmasının sağlanması; ve bilgilerin, sistemlerin gerektiğinde kullanıma hazır olmasının sağlanmasıdır. Bu nedenle tüm Arçelik ve dışkaynaklı personeller ile stajyerleri, bayi kullanıcıları ve yansanayi personeli konumları veya görevleri ne olursa olsun işlerini, bilgilerin Arçelik bünyesinde korunmasını gözetecek biçimde yapmaktan sorumludur.

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 BilgiGuvenligi@arcelik.com /informationsecurity@arcelik.com adresine bildirmek
- Bilgi sistemlerinin çalışmasını olumsuz etkileyebilecek veya bilgi güvenliğini tehlikeye atacak faaliyetlerde bulunmamak.

- Bilgi Güvenliği dokümanları ile ilgili güncelleme/iyileştirme taleplerini Bilgi Güvenliği Yöneticine 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 gözlemlemek ve güncelliğini sağlamak,
- Sahibi oldukları varlıkların Kişisel Verileri dahil olmak üzere sınıflandırmasını, güncellenmesini ve gözden geçirilmesini sağlamaktan sorumludur.

Arçelik personeli, Arçelik Personel Yönetmeliği Kurallarında belirtilen gizli bilgilerin korunması ve Arçelik Global İş Etiği İlkelerine de uymak zorundadır.

Arçelik; Kişisel Verilerin Korunması Yasasında belirtilen önlemleri almayı ve Koç Holding Kişisel Verilerin Korunması Politikasına tam uyumlu çalışmayı taahhüt eder.

Üçüncü Partiler

Arçelik'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 Arçelik Politika ve Prosedürleri'ne uygun hareket etmek.
- Arçelik'e ait bilgi ve varlıkları Arçelik onayı ve izni olmadan başkaları ile paylaşmamak.
- Arçelik tarafından kendilerine verilen kimlikleri mukavelelere ve talimatlara uygun şekilde kullanmak
- Üçüncü partinin Arçelik'le çalışmakta olan çalışanlarının kendi firmasından ayrılması/görev değiştirmesi söz konusu ise, bu durumu aynı gün içerisinde Arçelik'e bildirmek ve yetkilerinin iptal edilmesini sağlamak.
- Arçelik'in onay ve izni olmadan, Arçelik'in cihazınlarındaki hiçbir veri ve yazılımı kopyalamamak, ortamın ses kaydınını almamak, resmini, videosunu çekmemek, veri güvenliğini veya imajını tehlikeye atabilecek paylaşımlarda/hareketlerde bulunmamak.

Arçelik lokasyonlarında yapılacak sistem erişimlerini Bilgi Teknolojileri ekiplerinin gözetiminde gerçekleştirmek.

3. Politika Sahipliği ve Bilgi Güvenliğinde Rehberlik Sağlanması

Bu politikanın ve tüm standartların ve diğer destekleyici belgelerin ve eğitim faaliyetlerinin işlevsel sahipliği BT Güvenlik Yöneticiliği tarafından yürütülecek ve bu yöneticilik, aynı zamanda politikanın tüm Arçelik bünyesinde uygulanmasıyla ilgili olarak tavsiye kaynağı ve rehber olacaktır.

BT Güvenlik Yöneticiliği tüm çalışanların, Bilgi Güvenliği konularıyla ilgili uygun bilinçlenme düzeyinin oluşmasını sağlayacak uygun eğitimleri almalarını temin edecek ve genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik edecektir. Gerekli olduğunda bu politikanın ayrıntılı standartlar, prosedürler ve süreçlerle desteklenmesini ve bunların gerek doğdukça kullanıma hazır olmasını sağlayacaktır. Ayrıca bu politika gereklerinin tüm çalışanlara (daimi veya dönemsel) ve tüm yüklenici personeline aktarılmasını sağlamaktan sorumlu olacaktır.

Üst Yönetim, Bilgi Güvenliği ile ilgili genel yönetim çerçevesinin oluşturulmasından, sürekliliğinin sağlanmasından, bu politikanın, güncel olarak yaşamasını ve Arçelik 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.

Bilgi Güvenliği politikaları Arçelik bilgi varlıklarının karşı karşıya olduğu güncel riskleri yansıtması amacıyla yapılan varlık ve risk güncellemelerine paralel olarak yılda en az bir defa gözden geçirilirler. Yeni riskleri ve risklerde meydana gelen değişiklikleri kontrol altında tutmak için Bilgi Güvenliği Politikaları gerekli eklemeler yapılarak güncellenir. Ayrıca herhangi bir Arçelik çalışanı Bilgi Güvenliği Politikaların gelişmesi ve Arçelik'nun ihtiyaç duyduğu kontrolleri daha iyi yansıtması amacıyla politikaların değiştirilmesi konusunda BT Güvenlik Yöneticiliğine talepte bulunabilir. Yapılan talepler BT Güvenlik Yöneticiliği tarafından ele alınır ve değerlendirilir.

Bilgi Güvenliği Politikası ilkeleri, Arçelik İnsan Kaynaklarının Personel Yönetmeliği Kurallarına paralel uygulanmalıdır. Çalışanlar ayrıca Bilgi Güvenliği Politikasının farkında olmaktan ve bu ilkelere uymaktan sorumludur.

4. Denetleme ve Politikalara Uyulması ve Uyulmama Durumlarının Çözümlenmesi

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

BT Güvenlik Yöneticiliği başta Bilgi Güvenliği Politikası olmak üzere yayınlanmış olan tüm politika ve prosedürler ile ilgili standartlara uyumun periyodik olarak denetiminden ve ilgililere raporlanmasından sorumludur.

Bilgi Güvenliği Politikası ihlalleri, Arçelik'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 Arçelik 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 sonuçlanabilecektir.

Bu politikanın uygulanması konusunda hep birlikte çalışılması, bilgilerimizin ve itibarımızın sürekli olarak korunmasına ve işimizin başarısının devamlılığının sağlanmasına yardımcı olacaktır.

5. Hedefler

Arçelik Bilgi Güvenliği, Arçelik'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 bilinç, 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,
- En güncel ve etkin teknik güvenlik kontrolleri uygulamayı hedefler.

Tüm çalşanlar bu hedeflere katkı sağlamaktan sorumludur.