

1. Politika

Emko Elektronik San. ve Tic. A.Ş' de bilgi güvenliğinin amacı Emko Elektronik San. ve Tic. A.Ş' nin varlıklarını, müşteri verilerini ve bilgi sistemlerini siber tehditlere karşı korumak için açık ve kapsamlı bir çerçeve oluşturmaktır. Emko Elektronik San. ve Tic. A.Ş' nin bilgi güvenliği ve siber güvenlik gereksinimlerini, önemini ve uygulamasını tanımlama amacıyla yürütülen bilgi güvenliği yönetimi aktiviteleri için formal bir metodoloji oluşturmaktır. Siber tehditlere karşı güvenli ve dirençli bir altyapı oluşturulması ve sürdürülmesi, kurum ve müşteri bilgilerinin güvenliğinin sağlanması, müşteri güveninin korunması konularında kararlılığını özetlemektedir.

Bilgi; kurum ve kuruluşların faaliyetlerini gerçekleştirmesi için gerekli olan, çeşitli ortamlarda bulunabilen değerli bir kaynaktır. Emko Elektronik San. ve Tic. A.Ş edinilen, saklanan, taşınan tüm bilgilerin uygun koşullarda korunmasını hedeflemektedir.

Emko Elektronik San. ve Tic. A.Ş' de Bilgi Güvenliği; iş sürekliliğini sağlamak, finansal ve operasyonel kayıpları en aza indirmek amacıyla bilgi varlıklarının tehditlere karşı korunması olarak tanımlanır. Bilgi güvenliği ile saklanan, işlenen veya iletilen her türlü bilginin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması hedeflenir.

Bu politikanın temel amacı; kurumsal veri ve bilgi varlıklarımızı her türlü iç ve dış tehdide karşı korumak, yasal mevzuatlara (KVKK vb.) tam uyum sağlamak ve şirketimizin dijital güvenliğini en üst düzeyde tesis etmektir.

2. Kapsam

Bu politika, Emko Elektronik San. ve Tic. A.Ş bilgi varlıklarını, bilgi sistemleri süreçleri ve altyapısını, tüm çalışanları, üçüncü parti tedarikçileri, danışmanları, kurum sistemlerine, verilerine veya teknoloji kaynaklarına erişimi olan tüm paydaşları kapsar. Politikada yer alan kural ve esaslara çalışanlarımız tarafından istisnasız uyulması, kurumsal güvenilirliğimizin korunması adına önemlidir.

Tüm çalışanlar ve tedarikçiler, ülkemizdeki yasal mevzuatlar, ilgili yasa ve yönetmeliklere uymakla yükümlüdür. Bu amaçla bilgi sistemlerini kullanan, yöneten ve bilgi kaynaklarına erişen herkes;

- Bilgi varlıklarının gizlilik, bütünlük ve kullanılabilirliğini korumak,
- Bilgi güvenliği ve siber güvenlik politika, standart, prosedür ve talimatlarını bilmek ve uygulamak,
- BT kaynaklarını yasalara, politikalara ve iş amaçlarına uygun kullanmak,
- Müşteri bilgilerinin gizliliğini ve mahremiyetini sağlamak,
- Bilgiyi sadece yetkili kişiler ile paylaşmak,
- Tahmin edilmesi zor şifreler kullanmak ve gizliliğini sağlamak
- Bilginin uygun şekilde yedeklenmesini ve iş sürekliliğini sağlamak,
- Bilgi güvenliği ihlal olaylarını ve potansiyel zayıflıkları raporlamak zorundadır.

Doküman No:	Yayın Tarihi:	Revizyon No:	Revizyon Tarihi:	Sayfa No:
E-KGM-PLTK-014	30.11.2025	00	-	1 / 4
Hazırlayan		Onay		
Kalite Sorumlusu		Genel Müdür		

*Bu doküman elektronik ortamda günceldir. Basılmış hali, yayınlayan birim tarafından onaylanmadıkça **KONTROLSÜZ KOPYA**' dır.*

3. Rol ve Sorumluluklar

Yönetim Kurulu

Politikaya, kural ve düzenlemelere uyulmaması durumunda bildirim aldığı, yaptırım mekanizmalarının belirlenmesi ve işletilmesinin üst gözetiminden sorumludur.

Bilgi İşlem Sorumlusu

Bilgi İşlem (IT) Birimi, siber güvenlik altyapısının kurulması, işletilmesi ve denetlenmesinden sorumludur. Birim, şirket verilerini korumak adına aşağıdaki önlemleri almayı ve uygulamayı taahhüt eder:

Teknik Altyapı Yönetimi: Güvenlik duvarı (firewall), antivirüs sistemleri ve siber atak tespit/engelleme yazılımlarını 7/24 aktif, çalışır ve güncel durumda tutar.

Erişim ve Yetkilendirme: Personelin kurumsal verilere erişimini "En Az Yetki Prensibi" (Least Privilege) çerçevesinde düzenler; her çalışana sadece görevinin gerektirdiği ölçüde erişim izni tanımlar.

Veri Yedekleme ve Kurtarma: Kritik sistemlerin ve verilerin düzenli olarak yedeklenmesini sağlar, bu yedekleri olası siber saldırılardan (fidyecilik/ransomware yazılımları dahil) etkilenmeyecek şekilde izole edilmiş güvenli alanlarda muhafaza eder.

Risk Analizi ve Taahhüt: Yılda en az bir kez olmak üzere periyodik olarak siber güvenlik risk analizlerini gerçekleştirir. Tespit edilen güvenlik açıklarını hızla kapatarak olası siber riskleri minimum seviyeye indirmeyi taahhüt eder.

İş Sürekliliği ve Acil Durum Planları: Bilgi İşlem birimi tarafından oluşturulur, güncelliği sağlanır.

Veri Yedekleme Prosedürleri/Talimatları: Bilgi İşlem birimi tarafından oluşturulur, güncelliği sağlanır.

Virüs ve Saldırganlardan Korunma Talimatları: Bilgi İşlem birimi tarafından oluşturulur, güncelliği sağlanır.

Bilgi Güvenliği ve İhlal Bildirim formu: Kayıtları toplar, değerlendirir, gerekli önlemleri alır ve raporlar.

Eğitim ve Gelişim Zorunluluğu: Bilgi İşlem Birimi göreve yeni başlayan her personele, işbaşı yaptığı ilk hafta içerisinde kapsamlı bir Bilgi güvenliği ve siber güvenlik oryantasyon eğitimi verir. Ayrıca siber güvenlik dünyasındaki güncel tehditler ve yeni teknolojiler hakkında, birim personeline yönelik periyodik e-mail bilgilendirmeleri yapar veya eğitimler düzenler.

- Politikanın yürütülmesinden, güncellemesinden ve geliştirilmesinden,
- Politikaya uyum için gerekli teknik tedbirlerin alınmasından,
- Görev alan çalışanlarla beraber tedbirlerin uygulanmasından,
- Politikaya aykırı durumlarda Yönetim Kurulu'na gerekli bildirimlerin yapılmasından,
- Güncel Dokümanların web sitesinde yayınlanmasından sorumludur.
- Sır saklama yükümlülüğü işten ayrılma dahi sınırsız süreyle geçerlidir.

Departman Sorumluları

Departman yöneticileri, sevk ve idare ettikleri birimlerde güvenlik kültürünün yerleşmesinden ve sürdürülmesinden sorumludur. Aşağıdaki önlemleri almayı ve uygulamayı taahhüt eder:

İnsan Kaynakları Koordinasyonu: Yeni başlayan veya iş akdi sonlandırılan personelin yetkilendirme süreçlerini (hesap açma/kapatma) Bilgi İşlem Birimi ile anlık olarak koordine eder.

Uyum Denetimi: Kendi ekiplerinin bu politikada yer alan kurallara tam uyumunu düzenli olarak gözlemler ve denetler.

Doküman No:	Yayın Tarihi:	Revizyon No:	Revizyon Tarihi:	Sayfa No:
E-KGM-PLTK-014	30.11.2025	00	-	2 / 4
Hazırlayan	Onay			
Kalite Sorumlusu	Genel Müdür			

*Bu doküman elektronik ortamda günceldir. Basılmış hali, yayınlayan birim tarafından onaylanmadıkça **KONTROLSÜZ KOPYA** dır.*

- Görev alan çalışanlarla beraber tedbirlerin uygulanmasından,
- Politikaya aykırı durumlarda Yönetim Kurulu'na gerekli bildirimlerin yapılmasından sorumludur.
- Sır saklama yükümlülüğü işten ayrılrsa dahi sınırsız süreyle geçerlidir.

Çalışanlar

Şirkete ait bilişim altyapısını ve verileri kullanan tüm personel, aşağıdaki kurallara ve sorumluluklara uymayı taahhüt eder:

Kimlik Doğrulama Güvenliği: Kullanıcı hesaplarında kurumsal standartlara uygun güçlü şifreler kullanır. Şifrelerini üçüncü kişilerle veya mesai arkadaşlarıyla hiçbir surette paylaşmaz.

Temiz Masa ve Temiz Ekran İlkesi: Çalışma alanından uzaklaşırken bilgisayar ekranını kilitler. Çalışma masasında şifre, müşteri bilgisi veya gizli veri içeren fiziki evrak bırakmaz.

Cihaz ve Ağ Kullanım Kuralları: Şirket bilgisayarlarına Bilgi İşlem onayı olmayan harici depolama aygıtlarını (USB bellek vb.) takmaz. Lisanssız veya onaylanmamış yazılımları bilgisayarına yüklemeyiz. Şirket dışı çalışmalarda güvenli olmayan halka açık (kamusal) Wi-Fi ağlarını kullanmaz.

E-Posta ve Sosyal Mühendislik Güvenliği: Kaynağı doğrulanmamış, şüpheli veya olağan dışı talepler içeren e-postaların eklerini açmaz ve içerisindeki bağlantı linklerine tıklamaz.

AI Farkındalığı: Firma'nın yazılım, tasarım, ticari sır, finans vb. ve müşteri ile ilgili bilgilerini Yapay zeka programlarında paylaşılması gerektiğinin bilincindedir.

- Politikaya aykırı durumlarda Yönetim Kurulu'na gerekli bildirimlerin yapılmasından sorumludur.
- Sır saklama yükümlülüğü işten ayrılrsa dahi sınırsız süreyle geçerlidir.

4. Usulsüzlük ve İhlal Durumunda Yapılacak Bildirimler

Şirket güvenliğini tehlikeye atan usulsüz durumların ve güvenlik ihlallerinin erken tespiti, olası zararların büyümesini engellemek için kritik önem arz eder:

- Şüpheli Durum Bildirimleri:** Herhangi bir siber saldırı şüphesi, bilgisayarlarda tespit edilen olağan dışı hareketler veya şüpheli e-postalar karşılaşıldığı anda **gecikmeksizin** Bilgi İşlem Birimi'ne rapor edilir.
- Veri İhlali Şüphesi:** Şirkete ait gizli bilgilerin veya kişisel verilerin yetkisiz kişilerin eline geçtiğine dair bir şüphe oluşması durumunda, ilgili bölüm yöneticisi durumu derhal yazılı olarak Bilgi İşlem Sorumlusuna iletmekle yükümlüdür.
- Kötü Niyetli Kullanım ve Yaptırımlar:** Şirket güvenlik kurallarını kasıtlı olarak ihlal eden, kurumsal verileri yetkisiz üçüncü şahıslarla paylaşan veya sistemlerde usulsüzlük yaptığı tespit edilen personeller hakkında Departman Yöneticisi, Bilgi İşlem Yöneticisi ve İnsan Kaynakları birimi tarafından gerekli savunmalar alınır ve hukuki süreç başlatılır.

5. Dokümanın Yayınlanması ve Saklanması

İşbu Politika elektronik ortamda saklanır.

Doküman No:	Yayın Tarihi:	Revizyon No:	Revizyon Tarihi:	Sayfa No:
E-KGM-PLTK-014	30.11.2025	00	-	3 / 4
Hazırlayan		Onay		
Kalite Sorumlusu		Genel Müdür		

*Bu doküman elektronik ortamda günceldir. Basılmış hali, yayınlayan birim tarafından onaylanmadıkça **KONTROLSÜZ KOPYA** 'dır.*

6.Güncelleme Periyodu

İşbu Politika en az yılda bir kez gözden geçirilir ve ihtiyaç halinde Yönetimin Gözden Geçirme Toplantısında güncellenir.

7.Yürürlük

İşbu Politika Şirket internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

EKLER:

Bilgi Güvenliği ve İhlal Bildirim formu (Form_No:181)

Doküman No:	Yayın Tarihi:	Revizyon No:	Revizyon Tarihi:	Sayfa No:
E-KGM-PLTK-014	30.11.2025	00	-	4 / 4
Hazırlayan		Onay		
Kalite Sorumlusu		Genel Müdür		

*Bu doküman elektronik ortamda günceldir. Basılmış hali, yayınlayan birim tarafından onaylanmadıkça **KONTROLSÜZ KOPYA** 'dır.*