

# GİMAT MAĞAZACILIK SANAYİ VE TİCARET A.Ş.

## BİLGİ SİSTEMLERİ GÜVENLİĞİ POLİTİKASI

### 1. Amaç

Bu Politikanın amacı, Gimat Mağazacılık Sanayi ve Ticaret A.Ş.'nin sahip olduğu bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak, bilgi güvenliği risklerini yönetmek ve siber tehditlere karşı gerekli önlemleri almaktır.

### 2. Kapsam

Bu politika;

- Tüm çalışanları,
- Yönetim Kurulu üyelerini,
- Danışmanları,
- Tedarikçileri,
- Dış hizmet sağlayıcıları,
- Fiziksel ve elektronik bilgi varlıklarını

kapsamaktadır.

### 3. Bilgi Güvenliği Hedefleri

Şirket;

- Bilgi varlıklarını korumayı,
- Yetkisiz erişimleri önlemeyi,
- Siber riskleri azaltmayı,
- Yasal yükümlülüklerle uyumu sağlamayı,
- Operasyonel sürekliliği korumayı hedefler.

### 4. Bilgi Varlıklarının Korunması

Şirket bünyesindeki;

- Finansal veriler,
- Müşteri bilgileri,
- Ticari sırlar,
- Kurumsal belgeler,
- İnsan kaynakları verileri,
- Elektronik kayıtlar

kurumsal bilgi varlığı olarak kabul edilir ve korunur.

## 5. Eriřim Kontrolleri

- Kullanıcılara yalnızca görevleri kapsamında yetki verilir.
- Ortak kullanıcı hesapları kullanılmaz.
- Güçlü parola kuralları uygulanır.
- Kritik sistemlerde çok faktörlü kimlik doğrulama uygulanır.
- Yetkiler düzenli olarak gözden geçirilir.

## 6. Ağ ve Sistem Güvenliđi

řirket;

- Güvenlik duvarı sistemleri kullanır,
- Antivirüs ve zararlı yazılım koruması sağlar,
- Sistem güncellemelerini düzenli gerçekleştirir,
- Ağ trafiđini izler,
- Kritik sistemleri koruma altına alır.

## 7. Veri Yedekleme

- Kritik veriler düzenli olarak yedeklenir.
- Yedekler güvenli ortamlarda saklanır.
- Yedeklerden geri dönüş testleri periyodik olarak yapılır.

## 8. Olay Yönetimi

Bilgi güvenliđi olayları;

- Derhal raporlanır,
- Kayıt altına alınır,
- Analiz edilir,
- Gerekli düzeltici faaliyetler uygulanır.

## 9. Siber Güvenlik

řirket;

- Siber tehditleri izler,
- Güvenlik testleri gerçekleştirir,
- Zafiyet analizleri yapar,
- Güvenlik açıklarını giderir,
- Olay müdahale planlarını güncel tutar.

## 10. Çalışan Sorumlulukları

Çalışanlar;

- Bilgi güvenliđi kurallarına uymak,
- Şifrelerini korumak,

- Şüpheli durumları bildirmek,
- Şirket verilerini yetkisiz kişilerle paylaşmamak

ile yükümlüdür.

## 11. Eğitim ve Farkındalık

Şirket çalışanlarına düzenli olarak;

- Bilgi güvenliği,
- Siber güvenlik,
- Sosyal mühendislik,
- Veri koruma

konularında eğitim verilir.

## 12. İhlaller ve Yaptırımlar

Bu politikaya aykırı davranışlar disiplin süreçleri kapsamında değerlendirilir ve gerekli idari işlemler uygulanır.

## 13. Yürürlük

Bu politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer ve yılda en az bir kez gözden geçirilir.