DAĞITIM

Elektronik ortamda tüm kullanıcılara açıktır. Bu prosedürün güncellenmesi Bilgi İşlem Bölümü yetki ve sorumluluğundadır.

REVİZYON GEÇMİŞİ	TANIM	TARİH
0	Politikanın oluşturulması	31.12.2025

HAZIRLAYAN: BGYS SORUMLUSU	ONAYLAYAN: GENEL MÜDÜR

1.Amaç

Bu politikanın amacı, Katmerciler A.Ş.'nin bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumak; bilgi güvenliği risklerini yönetmek ve bilgi sistemlerinin güvenli bir şekilde işletilmesine ilişkin esasları belirlemektir.

Bu politika, şirket bünyesinde uygulanmakta olan **ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi** ile uyumlu olarak hazırlanmış olup, ayrıca **Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği** kapsamında uygulanır.

2.Kapsam

Bu politika;

- Şirketin tüm bilgi varlıklarını,
- Bilgi sistemlerini, yazılımları ve altyapıyı,
- Elektronik veya fiziksel ortamda tutulan verileri,
- Bu bilgilere erişimi olan çalışanları, yöneticileri ve üçüncü tarafları

kapsar.

3. Dayanak ve İlgili Mevzuat

Bu politika aşağıdaki mevzuat ve standartlara dayanılarak hazırlanmıştır:

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- SPK VII-128.10 Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği
- 6698 sayılı Kişisel Verilerin Korunması Kanunu

4. Bilgi Güvenli Sorumlusu Ataması

Bilgi güvenliği sorumlusu belirleme ve çalışma kriterleri belirlenmiştir.

- Bilgi güvenliği altyapıları ve yönetimi konusunda bilgi sahibi olmalıdır.
- Riskler ve risklerin yönetimi konusunda bilgi ve deneyimi bulunmalıdır.
- Bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye sahip olmalıdır.
- En az 5 yıl tecrübesi olmalıdır.
- Bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi konusunda görev üstlenmeyecektir.
- Üst yönetime bağlı olarak çalışacaktır.

5. Temel Bilgi Güvenliği İlkeleri

Bilgi güvenliği faaliyetleri aşağıdaki temel ilkeler doğrultusunda yürütülür.

5.1 Gizlilik

Bilgi varlıklarına yalnızca yetkili kişiler erişebilir. Yetkisiz erişimler önlenir.

5.2 Bütünlük

Bilginin doğruluğu, tamlığı ve güncelliği korunur. Yetkisiz değişikliklere izin verilmez.

5.3 Erişilebilirlik

Yetkili kullanıcıların, görevlerini yerine getirebilmeleri için gerekli bilgilere ihtiyaç duydukları zamanda erişebilmeleri sağlanır.

6. Yönetim ve Sorumluluklar

6.1 Yönetim Kurulu

Bilgi güvenliği ve bilgi sistemlerinin yönetimine ilişkin nihai sorumluluk Yönetim Kurulu'na aittir. Yönetim Kurulu, bilgi güvenliği politikalarının uygulanmasını ve etkinliğini gözetir.

6.2 Üst Yönetim

Üst yönetim, bilgi güvenliği süreçlerinin etkin şekilde uygulanmasını sağlar ve gerekli kaynakları temin eder.

6.3 Bilgi Güvenliği Sorumlusu

Bilgi Güvenliği Sorumlusu;

- Bilgi güvenliği uygulamalarını koordine eder,
- Bilgi güvenliği risklerini ve olaylarını izler,
- Gerekli durumlarda üst yönetime ve Yönetim Kurulu'na raporlama yapar.

6.4 Çalışanlar ve Üçüncü Taraflar

Tüm çalışanlar ve bilgi varlıklarına erişimi olan üçüncü taraflar, bu politika ve ilgili prosedürlere uymakla yükümlüdür.

7. Risk Yönetimi ve Süreçleri

7.1 Risk Yönetimi

Bilgi güvenliğine ilişkin riskler, ISO/IEC 27001 kapsamında belirlenen risk yönetimi metodolojisi doğrultusunda düzenli olarak değerlendirilir.
Risk değerlendirmesi, **sermaye piyasası faaliyetlerini destekleyen bilgi sistemlerini ve SPK VII-128.10 Tebliği kapsamındaki riskleri** de içerir.

7.2 Risk Değerlendirmesi ve Analizi

- Bilgi güvenliğine ilişkin risk kriterleri belirlenmiştir ve en az yılda bir defa gözden geçirilmektedir.
- Riskli olan faaliyetler listesi hazırlanmıştır ve yılda en az bir defa gözden geçirilmektedir.
- Risk olasılık ve etki analizleri yapılmaktadır.

8. Sürekli İyileştirme

Sürekli iyileştirme planımız bulunmakta ve güncellenmektedir. Plan içerisinde gerekli kaynak, hedef tarih gibi kayıtlar tutulmaktadır. Hedeflenen tarihte iyileştirmenin yapılamadığı durumlarda, denetim ve analizlerde ele alınmaktadır.

9. Eğitim ve Denetim

Uygun eğitim dönemleri belirlenmekte ve farkındalık eğitimleri planlanmaktadır. Planlanan eğitimler ile personelin bilgi güvenliği konusunda farkındalığın oluşması veya artırılması hedeflenmektedir.

Firma içerisinde belirlenen iç denetçiler aracılığıyla her yıl iç denetimlerimiz yapılmaktadır. İç denetimlerde soru listeleri üzerinden bilgi güvenliği konuları denetlenmekte, varsa uygunsuzluklar ile ilgili dif düzenlenmekte ve gerekli düzeltmeler yapılmaktadır.

10. Bilgi Güvenliği Olayları

Bilgi güvenliği olayları derhal Bilgi Güvenliği Sorumlusu'na bildirilir.
Önemli bilgi güvenliği olayları, gerekli görülen hallerde üst yönetime ve Yönetim Kurulu'na raporlanır.

11. Dış Kaynak Kullanımı

Bilgi sistemlerine ilişkin dış kaynaklı hizmetlerde;

- Bilgi güvenliği gereklilikleri sözleşmelerle güvence altına alınır,
- Gizlilik ve veri güvenliği hükümlerine yer verilir,

12. Yürürlük ve Gözden Geçirme

Bu politika **Yönetim Kurulu onayı** ile yürürlüğe girer.
Politika, yılda en az bir kez veya gerekli görülen hallerde gözden geçirilir.