BİM BİRLEŞİK MAĞAZALAR A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

BİM Bilgi Güvenliği Politikasının esaslı hususlarına aşağıda yer verilmiştir.

Bilgi Güvenliği Politikası, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konan VII128.9 Bilgi Sistemleri Yönetimi Tebliği (Tebliğ), konuyla ilgili Kişisel Verilerin Korunması Kanunu ve diğer düzenlemeler dikkate alınarak hazırlanmıştır.

1. AMAÇ

BİM'in bilgi güvenliğini yönetmekteki amacı; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden ve/veya dışarıdan gelebilecek, kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunması ve yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesini temin etmektir.

Bilgi güvenliği politikasının amacı ise, tüm ilgili taraflara BİM bilgi güvenliği gereksinimlerinin bildirilmesi ve yazılı kuralların temel dayanağının oluşturulmasıdır.

2. KAPSAM

BİM Bilgi Güvenliği Yönetim Sistemi BİM'in tüm varlık ve teknolojilerini kapsamaktadır.

3. SORUMLULUK

Yönetim Kurulu

Bu politikada belirlenen kontrollerin ve bu politika doğrultusunda hazırlanacak prosedürlerin etkinliği ve yeterliliği Yönetim Kurulu sorumluluğundadır.

Üst Yönetim

Bu politikanın uygulama ve yürütme sorumluluğu bilgi sistemlerinin yönetiminden sorumlu birim(ler)in bağlı olduğu Üst Yönetim kademesidir. İlgili üst yönetim kademesi, bilgi güvenliği politikasının uygulanması için gerekli kaynakları sağlar.

Bilgi işlem Direktörlüğü

Bilgi Sistemleri risk yönetimi süreçlerinin, kontrollerinin ve gözetim mekanizmasının tanımlanmasından sorumludur.

Birim Yöneticileri

Bilgi Güvenliği Politikasını uygulamak ve çalışanlarının esaslara bağlılıklarını sağlamaktan sorumludur.

Tüm Bim Çalışanları

Bilgi Güvenliği Politikası ve kurallarını bilmek; bu kural ve esaslara uygun davranmak, güvenlik ihlallerini bildirmekten sorumludur.

Sözleşmeli Tedarikçiler/İş Ortakları

Sözleşmeli tedarikçiler ve/veya iş ortakları, bu esasa ve bu esas ile yürürlüğe konularak uygulanan politika, prosedür ve talimatlarına uymaktan sorumludurlar.

4. HEDEFLER

Bilgi Güvenliği Yönetim Sistemi şartlarını yerine getirerek, çalışanların bilgi güvenliği farkındalıklarını arttırmak, teknik güvenlik kontrollerini uygulamak ve kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, kurumsal riskleri en alt seviyeye indirerek kurumun güvenliği ile güvenilirliğini ve temsil ettiği kurumun imajını korumaktır.

5. ESASLAR

Her türlü bilgi; en az kesintiyle hizmet alanlar, hizmet verenler ve üçüncü taraflarca yetkileri dahilinde erişilebilir.

Bilgilerin gizliliği, bütünlüğü ve erişilebilirliğinin sürekli olarak sağlanması için gerekli çalışmalar yapılır.

Hizmet alanlar ve verenler ya da üçüncü taraflara ait olmasına bakılmaksızın, üretilen ve/veya kullanılan bilgilerin gizliliği her durumda güvence altına alınmaktadır.

Uygun kullanım kontrolü "**Güvenlik Standartlarına Uygun Kullanım Prosedürü**"nde ortaya konmuş esaslara göre sağlanır ve bilgi yetkisiz erişime karşı korunur.

Taşınabilir Bilgisayar kullanım kontrolü "**Bim Taşınabilir Bilgisayar Kullanım Prosedürü**"nde ortaya konmuş esaslara göre sağlanacak ve bilgi yetkisiz erişime karşı korunacaktır.

T.C. yasaları, yönetmelikler, genelgeler ve sözleşmeler ile belirlenmiş gereksinimler karşılanacak, bunlar ile uyumlu çalışma sağlanacaktır.

Kritik iş süreçlerini büyük felaketlerin ve işletim hatalarının etkilerinden korumak amacıyla iş sürekliliği yönetimi uygulanacaktır.

Personelin bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını teşvik edecek eğitimler düzenli olarak şirket çalışanlarına ve yeni işe giren çalışanlara sağlanacaktır.

Tüm birim yöneticileri bu esasların uygulanmasından birinci derecede sorumlu olacaklar ve personelinin esaslara uygun olarak çalışmasını sağlayacaktır.

6. GÖZDEN GEÇİRME

Bilgi Güvenliği Politikası organizasyonel değişiklikler, iş şartları, yasal ve teknik düzenlemeler vb. nedenlerle günün koşullarına uyumluluk açısından değerlendirilir.

Bu esaslar düzenli olarak, yılda en az bir (1) kez gözden geçirilir ve yapılan değişiklikler yönetim kurulu onayına sunulur. Prosedürlerde yapılacak değişiklikler ise üst yönetimin onayıyla hayata geçirilebilir.