1. Amaç

Bu politika, **İmam Kayalı Holding** bünyesindeki tüm bilgi varlıklarının **gizlilik, bütünlük ve erişilebilirliğini** korumak, Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulmasını, uygulanmasını, sürdürülmesini ve sürekli iyileştirilmesini sağlamak amacıyla hazırlanmıştır.

2. Kapsam

Bu politika, **İmam Kayalı Holding'in General Tekstil ve Enka Hijyen** şirketleri dahil olmak üzere tüm lokasyonlarını / tesislerini, birimlerini, bilgi sistemlerini, fiziksel ve elektronik bilgi varlıklarını, tüm çalışanlarını (tam zamanlı, yarı zamanlı, sözleşmeli) ve ilgili tüm üçüncü tarafları kapsar.

3. Bilgi Güvenliği Temel İlkeleri

İmam Kayalı Holding bilgi güvenliğini sağlamak için aşağıdaki temel ilkeleri benimser:

- **Gizlilik:** Bilginin yetkisiz kişilere, kuruluşlara veya süreçlere açıklanmasını önlemek. Hassas ve kritik bilgilerin sadece yetkili kişilerce erişilebilir olmasını sağlamak.
- **Bütünlük:** Bilginin doğruluğunu, tamlığını ve yetkisiz değiştirilmelere karşı korunmasını sağlamak. Bilgi işleme yöntemlerinin güvenilirliğini güvence altına almak.
- **Erişilebilirlik:** Yetkili kullanıcıların, iş süreçlerinin gerektirdiği anda ve şekilde bilgi ve ilişkili kaynaklara erişebilmesini sağlamak.

4. Kurumsal Taahhütler

İmam Kayalı Holding Üst Yönetimi, BGYS'nin etkinliğini sağlamak için aşağıdaki taahhüt eder:

- **Yasal ve Sözleşmesel Uygunluk:** Bilgi güvenliği ile ilgili tüm ulusal ve uluslararası yasal gerekliliklere, düzenlemelere ve müşterilerle yapılan sözleşmelerden doğan yükümlülüklere uymayı taahhüt etmek.
- **Risk Yönetimi:** Bilgi varlıklarını tanımlamak, risk değerlendirmesi metodolojisi belirlemek ve bilgi güvenliği risklerini kabul edilebilir seviyelere indirmek için gerekli kontrol önlemlerini uygulamak.
- **İş Sürekliliği:** Kritik iş süreçlerinin kesintiye uğramamasını sağlamak ve bilgi güvenliği olayları sonrasında hızlı ve etkin bir şekilde kurtarma sağlamak amacıyla iş sürekliliği ve acil durum planları geliştirmek ve test etmek.
- **Eğitim ve Farkındalık:** Tüm çalışanlara, bilgi güvenliği sorumluluklarını anlamaları ve BGYS'ye uyum sağlamaları için düzenli eğitim ve farkındalık faaliyetleri sunmak.
- **Sürekli İyileştirme:** BGYS'nin performansını izlemek, ölçmek ve sistemin amaçlarına uygunluğunu, doğruluğunu ve etkinliğini sürekli iyileştirmek.
- **Kaynak Sağlama:** BGYS'nin başarılı bir şekilde yürütülmesi için gerekli olan insan kaynağı, teknolojik altyapı ve finansal kaynakları sağlamak.

5. Detaylı Kontrol Alanları ve Gereklilikler

İmam Kayalı Holding belirlenen bilgi güvenliği risklerini yönetmek için aşağıdaki kontrol alanlarında detaylı gereklilikleri uygular:

5.1 Organizasyonel Gereklilikler

- **BGYS Yapısı:** BGYS'nin yönetiminden **BGYS Yöneticisi/BGYS Komitesi** sorumludur. İlgili tüm roller ve sorumluluklar BGYS görev tanımlarında belirtilmiştir. BGYS Komitesi 6 ayda bir toplantı düzenleyerek riskleri gözden geçirir. Olay/ihlal bildirimleri inceler gerekli aksiyonların alınmasını sağlar.
- **Bağımsız Gözden Geçirme:** BGYS'nin uygunluğu ve etkinliği, yılda bir yapılan **iç denetimler** ve **Yönetimin Gözden Geçirme Toplantısı ile değerlendirilir.**
- **Bilgi Güvenliği Olay Yönetimi:** Bilgi güvenliği olaylarının (ihlal, şüpheli faaliyet vb.) bildirimi, analizi ve çözümü **BGYS Olay Yönetimi Talimatında** belirtildiği şekilde ile yönetilir.

5.2 İnsan Kaynakları Güvenliği

- **İşe Alma Süreci:** Yeni çalışanlar için, rollerinin hassasiyetine uygun olarak **aday geçmiş sorgulama (tarama), referans kontrolü, adli sicil sorgulaması** gibi kontroller yapılacaktır.
- **Gizlilik Anlaşmaları:** Tüm çalışanlar, sözleşmeli personel ve ilgili üçüncü taraflar **Gizlilik Anlaşması** imzalamakla yükümlüdür.
- **İşten Ayrılma Süreci:** İK tarafından Bilgi İşlem'e bildirilen işten ayrılacak personel bilgisi ile personelin zimmetindeki bilgi varlıkları ve erişimi izlenir, personelin bilgi varlıklarına ve sistemlere erişimi, son iş gününde derhal ve sistematik olarak İK prosedürlerine uygun olarak iptal edilir.

5.3 Varlık Yönetimi

- **Varlık Envanteri:** Tüm kritik bilgi varlıklarının (veri tabanları, yazılımlar, donanımlar, fiziksel dokümanlar) envanteri Varlık Yönetimi ve Risk Değerlendirme talimatına uygun olarak güncel tutulur.
- **Varlık Sahipliği:** Her bilgi varlığına, varlığın güvenliğinden sorumlu olacak bir **Sahip/Emanetçisi** atanmıştır. Sahipler, varlığın sınıflandırmasına karar verir. İşten ayrılma ve pozisyon değişikliklerinde bilgi varlıkları iade alınır.
- **Bilgi Sınıflandırması:** Bilgiler, hassasiyet düzeylerine göre **Çok Gizli**, **Gizli, Özel, Genel**, **Hizmete Özel,** olarak sınıflandırılır ve bu sınıflandırmaya uygun olarak işlenir ve saklanır.

5.4 Erişim Kontrolü

- **İş Gereksinimi Temelli Erişim:** Kullanıcılara sadece görevlerini yerine getirmek için **mutlaka ihtiyaç duydukları** kaynaklara erişim hakkı (Minimum Yetkilendirme Prensibi) verilir.
- **Kullanıcı Kimlik Doğrulaması:** Sistemlere erişim için güçlü parola gereksinimlerini ve kritik sistemlerde **İki Faktörlü Kimlik Doğrulama (2FA) veya Çok Faktörlü Kimlik Doğrulama (MFA)** kullanımını zorunludur.
- **Ayrıcalıklı Erişim:** Yüksek yetkili (yönetici/admin) erişimler, özel olarak izlenir, kısıtlanır ve sadece onaylanmış görevler için kullanılır.

5.5 Fiziksel ve Çevresel Güvenlik

- **Güvenli Alanlar:** Kritik sunucu odaları ve veri merkezleri, yetkili personelin erişimine kısıtlanmış ve **Kartlı geçiş sistemleri, biyometrik sensörler** gibi kontrollerle korunmuştur.

- **Çevre Koruma:** Bilgi işleme tesisleri, yangın, su baskını ve elektrik kesintisi gibi çevresel tehditlere karşı **Yangın söndürme sistemleri, UPS/Jeneratörler** ile korunur.
- **Donanım Güvenliği:** Mülkiyetteki tüm donanımlar, yetkisiz yer değiştirmeye veya hırsızlığa karşı fiziksel olarak korunur.

6. Politikanın İzlenmesi ve Sürekli İyileştirme

Bu politikanın tüm gerekliliklerinin uygulandığından emin olmak için:

- **İzleme ve Ölçüm:** Tüm güvenlik kontrolleri, **BGYS Performans Göstergeleri (KPI'lar)** kullanılarak düzenli olarak izlenir ve ölçülür.
- **İç Denetimler:** BGYS, planlı aralıklarla İç Denetim Prosedürüne göre denetlenir. Denetim bulguları, düzeltici faaliyetler için Üst Yönetime raporlanır.
- **Düzeltici ve Önleyici Faaliyet:** Tespit edilen uygunsuzluklar ve güvenlik zafiyetleri, kök neden analizi yapılarak Düzeltici/Önleyici Faaliyet Prosedürüne göre ele alınır ve tekrarını önleyici adımlar atılır.

7. Yönetimin Taahhüttü

İmam Kayalı Holding Üst Yönetimi olarak, bilgi güvenliğinin şirketimizin sürdürülebilirliği, itibarı ve müşteri güveninin temel taşı olduğunun bilincindeyiz. Bu politika belgesi, bu anlayışımızın somut bir ifadesidir.

Bu politikanın başarılı bir şekilde uygulanması, iş sürekliliğimizin ve rekabet gücümüzün en önemli güvencesidir. Bu nedenle, tüm çalışanlarımızın, iş ortaklarımızın ve tedarikçilerimizin bu politika ile belirlenen ilke, taahhüt ve kurallara titizlikle uymasını şart koşuyoruz.

Biz, Üst Yönetim olarak, bu politikanın hayata geçirilmesi ve sürekli iyileştirilmesi için gerekli tüm liderliği göstermeyi, örnek olmayı ve kaynakları (insan, teknoloji, bütçe) sağlamayı taahhüt ediyoruz.

Bilgi güvenliği ihlalleri veya politika ihlalleri ciddiyetle ele alınacak, gerekli disiplin ve idari tedbirler uygulanacaktır.

Tüm paydaşlarımızın bu kolektif çabaya katkısı ve sahiplenmesi için şimdiden teşekkür ederiz.

Yönetim Kurulu Başkanı
Hasan Mazıcıoğlu