BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Bu politika, **BELBİM Elektronik Para ve Ödeme Hizmetleri A.Ş.** Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulması, işletilmesi, gözden geçirilmesi, iyileştirilmesi, sürekliliğinin sağlanması ve Bilgi Güvenliği Yönetimi'nin tüm iş süreçlerine entegre edilmesi amacıyla hazırlanmıştır.

2. KAPSAM

Bu politika, **BELBİM Elektronik Para ve Ödeme Hizmetleri A.Ş.**'nin bilgi güvenliği ile ilgili tüm süreçlerini kapsamakta olup politikanın kapsamına tüm Kurum çalışanları, danışmanlık & hizmet alınan 3. (üçüncü) taraflar ve tüm bilgi varlıkları dâhildir.

3. UYGULAMA

3.1. Tüm Kurum personeli ve danışmanlık & hizmet alınan 3. (üçüncü) taraflar ilgili oldukları bilgi güvenliği politika ve prosedürlerini bilmek ve çalışmalarını bu standartlara uygun şekilde yürütmekten sorumludur.

3.2. Bu politika ile Kurum;

3.2.1. Bilgi sistemlerinin sürekliliğini tam olarak sağlamayı,

3.2.2. Personellerin; bilinç, farkındalık ve güvenlik gereksinimlerine uyum düzeylerini en üst seviyeye çıkarmayı,

3.2.3. 3. (üçüncü) taraflar ile yapılan sözleşmelere uygunluğun tam olarak tesis edilmesini sağlamayı,

3.2.4. Bilgi güvenliği ihlal olaylarını en aza indirmeyi ve bunları öğrenme fırsatına çevirmeyi,

3.2.5. Bilginin yasalara tam uyumlu üretilmesini, erişim sağlanmasını ve saklanmasını,

3.2.6. En güncel ve etkin teknik güvenlik kontrollerini uygulamayı hedefler.

3.3. Kurum aşağıda belirtilen konuların yerine getirilmesini benimsemiştir;

3.3.1. Bilgi varlıklarına yönelik risklerin tespit edilmesi ve sistematik bir şekilde risklerin yönetilmesi,

3.3.2. Bilgi güvenliği standartlarının gerekliliklerinin yerine getirilmesi,

3.3.3. Bilgi güvenliği ile ilgili tüm yasal mevzuata uyum sağlanması,

3.3.4. Bilgi Güvenliği Yönetim Sistemi'nin yaşatılması için sürekli iyileştirme fırsatlarının değerlendirilmesi ve çalışmaların gerçekleştirilmesi,

Hazırlayan	Gözden Geçiren	Kontrol Eden	Onaylayan
<HAZIRLAYAN_DEPARTMAN_ADI>	<KONTROL_GRUP_ACK>	<1_ONAY_POZ_TAN>	<SON_ONAY_POZ_TAN>
<ALAN10>			

3.3.5. Bilgi güvenliği farkındalığını artırmak için, teknik ve davranışsal yetkinlikleri gerçekleştirecek şekilde eğitimler gerçekleştirilmesi,

3.3.6. Bilgi Güvenliği Kurulu ile bu politikaya bağlı diğer alt politika ve prosedürlerin hazırlanması ve yayınlanması.

3.4. Bilgi güvenliği oluşturan tüm dokümanlar, ISO/IEC 27001:2022 standartlarına uygun olacaktır**.**

3.5. Kurum adına bilgi güvenliği sorumluluğu Teknoloji Genel Müdür Yardımcısı'nda olacaktır.

3.6. BGYS aktivitelerini yönetmek ve yönlendirmek için Kurum içinde BGK (Bilgi Güvenliği Kurulu) oluşturulacaktır.

3.7. Genel Müdür, BGK, BGS ve BGYS Uygulayıcı Ekibi'ni atayacak, gerekli kaynakları sağlayacak ve sürekli iyileştirme prensibiyle BGYS Uygulayıcı Ekibi faaliyetlerini sürdürecektir.

3.8. Yapılan çalışmaların ve uygulanan kontrollerin çıktıları, etkileri ve verimi değerlendirilecektir.

3.9. Yeni teknolojiler ve teknoloji değişikliklerinin etkileri izlenecektir.

3.10. Tüm bilgi varlıklarının resmi envanteri çıkartılacak, varlıklar uygun şekilde sınıflandırılıp Kurum'un iş ihtiyaçları göz önüne alınarak etiketlendirilecek ve tüm kritik bilgi varlıkları (bilişim, kâğıt, fiziksel, insan) uygun kontrollerle koruma altına alınacaktır.

3.11. Bilgi güvenliği kapsamında; bilgi varlıkları üzerindeki tüm riskler değerlendirilecek, risk indirgeme faaliyetleri, önlemler ve kontroller tanımlanacaktır.

3.12. Bilgi varlıklarının imhaları Çevre, Şehircilik ve İklim Değişikliği Bakanlığı yönetmelikleri ile ISO 27001:2022 standardının sürdürülebilirlik esaslarına göre yapılacaktır.

3.13. Bilgi işlenirken, iletilirken ve muhafaza edilirken; Gizlilik, Bütünlük ve Erişilebilirlik esas alınarak korunacaktır.

3.14. Tüm sistemler için kabul edilebilir seviyede güvenlik sıkılaştırması yapılacak ve düzenli olarak kontroller ve iyileştirmeler sağlanacaktır.

3.15. Düzenli ve sürekli yapılacak kontroller, zafiyet ve sızma testleri yardımıyla; ağ, sunucu, altyapı, yazılım ve iletişim cihazları üzerinde güvenlik kontrolü ve denetimi yapılacaktır, uygun önlemler alınacaktır.

3.16. İş sürekliliğinin sağlanması için gerekli önlemler alınacak, etki analizleri, felaket kurtarma planları oluşturulacak ve süreklilik testleri yapılacaktır.

3.17. Ödeme verileri ve hassasa müşteri verileri uygun kontrollerle koruma altına alınacaktır.

3.18. Fiziksel lokasyonların (giriş çıkış kapıları, ofis odaları, ürün teslim alma/verme alanları, depolar, vb.) güvenliğinin sağlanması için gerekli kontroller oluşturulacaktır.

3.19. BGYS'nin işleyişini ve etkinliğini kontrol etmek için bir bağımsız denetim kuruluşundan hizmet alınarak en az yılda 1 (bir) kere BGYS İç Tetkik'i gerçekleştirilecektir.

3.20. Kurum çalışanları için periyodik olarak bilgi güvenliği farkındalık eğitimleri organize edilecektir.

3.21. Kurum, Türkiye Cumhuriyeti Devleti kanunlarının tanımladığı tüm yasal hükümlere uymak zorunda olup, hiçbir Kurum çalışanı, Türkiye Cumhuriyeti Devleti'nin kabul ettiği bilgi güvenliği ile ilgili kanunlara aykırı bir aktivitede bulunmayacaktır.

3.22. Tüm bilgi güvenliği olaylarının bildirim ve yönetimi, **"Mavi Masa"** (mavimasa.belbim.istanbul) üzerindeki **"Bilgi Güvenliği"** başlığı üzerinden yapılacaktır. Bu güvenlik ihlallerinin gelecekte tekrar oluşmaması ve kısa zamanda çözümlenmesi için gerekli tedbirler alınacaktır.

3.23. Bilgi güvenliği politikaları, prosedürleri ve eklerine uyulmadığı durumlarda, **"Disiplin Yönergesi"** çerçevesinde; sözlü uyarıdan işin akdinin sonlandırılmasına kadar değişen disiplin işlemleri uygulanabilecek, 3. taraflar için de şartname ve sözleşmelerdeki ilgili yaptırım maddeleri uygulanacaktır.

3.24. **"Temiz Masa ve Temiz Ekran Politikası"** Kurum bazında uygulanacak, tüm personeller **"Kabul Edilebilir Kullanım Politikası"**nda belirlenen talimatlara ve sorumlu oldukları diğer dokümanlardaki talimatlara uyacaktır.

3.25. Yürürlükte olan bilgi güvenliği politika, prosedür ve diğer dokümanlar **"QDMS"** (qdms.belbim.istanbul) üzerinden yayınlanacak ve tüm personele e-posta ile duyurulacaktır.

Hazırlayan	Gözden Geçiren	Kontrol Eden	Onaylayan
<HAZIRLAYAN_DEPARTMAN_ADI>	<KONTROL_GRUP_ACK>	<1_ONAY_POZ_TAN>	<SON_ONAY_POZ_TAN>
<ALAN10>			