1. AMAÇ:

Bu politikanın amacı; temel bilgi güvenliği prensiplerini tanımlamak ve bu prensiplere üst yönetimin verdiği desteği ifade etmektir.

2. KAPSAM:

Bu politikanın kapsamı tüm organizasyon ve bilgi varlıklarıdır.

3. SORUMLULUKLAR:

3.1. Genel Müdür

Politikanın şirketin bilgi güvenliği ihtiyaçlarını karşılar nitelikte bulunmasından ve politikanın uygulanması için gerekli kaynak ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya politikada değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

3.2. BGYS Temsilcisi

Genel Müdür tarafından görevlendirilen BGYS Temsilcisi, Bilgi Güvenliği Politikasının şirket ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından sorumludur.

3.3. Tüm Personel

Bilgi Güvenliği Politikasının gereklerinin görev alanlarının gerektirdiği biçimde yerine getirilmekten sorumludur.

4. TANIMLAR

BGYS : Bilgi Güvenliği Yönetim Sistemi

Gizlilik : Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır.

Bütünlük : Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır.

Erişilebilirlik: Bilginin ihtiyaç duyulduğu her an kullanıma hazır olmasıdır.

5. UYGULAMA

Misyon :

Müşterilerimize yenilikçi, güvenilir ve yüksek kaliteli yazılım çözümleri sunarak, işletmelerinin dijital dönüşümünü hızlandırmak.

Vizyon :

Dünya genelinde birçok sektörde lider bir yazılım şirketi olmak ve müşterilerimizin işlerini dijitalleştirmelerine yardımcı olmak için sürekli olarak teknolojik yenilikler sunmak.

BGYS Politikası

- Bilgi varlıklarını yönetmek, varlıkların güvenlik değerlerini, ihtiyaçlarını ve risklerini belirlemek, güvenlik risklerine yönelik kontrolleri geliştirmek ve uygulamak
- Bilgi varlıkları, değerleri, güvenlik ihtiyaçları, zafiyetleri, varlıklara yönelik tehditlerin, tehditlerin sıklıklarının saptanması için yöntemlerin belirleyeceği çerçeveyi tanımlamak.
- Tehditlerin varlıklar üzerindeki gizlilik, bütünlük, erişilebilirlik etkilerini değerlendirmeye yönelik bir çerçeveyi tanımlamak.
- Risklerin işlenmesi için çalışma esaslarını ortaya koymak.
- Hizmet verilen kapsam bağlamında teknolojik beklentileri gözden geçirerek riskleri sürekli takip etmek
- Tabi olduğu ulusal veya uluslararası düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik şirket sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- Hizmet sürekliliğine yönelik bilgi güvenliği tehditlerinin etkisini azaltmak ve sürekliliğe katkıda bulunmak
- Gerçekleşebilecek bilgi güvenliği olaylarına hızla müdahale edebilecek ve olayın etkisini en aza indirecek yetkinliğe sahip olmak
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Tüm personele Bilgi Güvenliği Yönetim Sistemi Politikası, Süreçler vb. konularda farkındalık, bilgilendirme ve bilinçlendirme eğitimleri vermek. Bu eğitim belirli periyotlarda tekrarlamak.
- Bilgi Güvenliği Yönetim Sistemi kapsamındaki uygulama, denetim, düzeltici faaliyet sonuçlarını göz önünde bulundurarak, sistemi sürekli iyileştirmek.
- Bilgi Güvenliği Yönetim Sistemini firma bünyesindeki diğer yönetim sistemleriyle birlikte bütünleşik olarak yürütmek.
- Kişisel Verilerin Korunması Kanunu (KVKK) gereksinimlerini anlamak ve karşılamak için çalışmalar yapmak.
- Firma itibarını geliştirmek, bilgi güvenliği temelli olumsuz etkilerden korumak.

6. YAPTIRIM

Bu politikaya uygun olarak çalışmayan tüm personel hakkında **Disiplin Prosedürü** hükümleri uygulanır.

Revizyon Tarihçesi		
Revizyon Numarası	**Revizyon Tarihi**	**Revizyon Açıklaması**
00		İlk Yayın

	Sorumlu	**İmza**
Hazırlayan	Yönetim Temsilcisi	
Onaylayan	Genel Müdür	