

## ARAS DİJİTAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS) POLİTİKASI

Aras Digital olarak, güvenilirliğimizi ve verdiğimiz hizmetleri korumak adına faaliyetlerimizin, şirketimizin, çalışanlarımızın ve müşterilerimizin verilerinin güvenliğini gözeterek devam etmesini amaçlıyoruz.

Bu amaç doğrultusunda faaliyetlerimizi, yasalar, kargo sektörü mevzuatı, kurumsal normlarımız ve ISO/IEC 27001 şartları ile uyumlu olarak tasarımı, işletimi, geliştirilmesi ve sürdürülmesi adına bilgi güvenliğini sağlamayı hedefliyoruz.

Bilgi Güvenliği, Aras Digital bilgi varlıklarının bütünlük, erişilebilirlik ve gizlilik niteliklerinin korunmasıdır. Herhangi bir formatta veya şekilde bulunan, içerisinde kurumsal veya kişisel bilgi barındıran, Aras Digital'in taahhütlerini ve iş süreçlerini yerine getirmede kullanılan, fiziki veya dijital tüm varlıklar "bilgi varlığı" olarak tanımlanır.

- Bütünlük: Aras Digital bilgi varlıklarının tamlık ve doğruluk özelliklerinin korunmasıdır.
- Erişilebilirlik: Aras Digital bilgi varlıklarının sadece yetkilendirilmiş izinli kişiler, kurumlar veya süreçler için kullanılabilir olmasıdır.
- Gizlilik: Aras Digital bilgi varlıklarının yetkisiz izinsiz kişiler, kurumlar veya süreçler için erişilebilir olmamasıdır.

Aras Digital Yönetimi, BGYS Politikası ile Aras Digital şirket hedeflerine ulaşılması için, bilgi güvenliği amaçlarının gerçekleştirilmesini, BGYS 'nin sürekli iyileştirilmesini sağlayacak şartların ve kaynakların tahsisini, çalışanlarımızın farkındalığının artırılmasını, BGYS gereklerinin yönetimini ve kontrolünü sağlayacağını taahhüt eder.

Aras Digital bilgi güvenliği amaçları, bilgi güvenliği risk değerlendirme süreci çıktılarına uygun olarak oluşturulur.

Aras Digital'in çalışanları olarak aşağıdaki ilkeleri uygulamak ve desteklemek üzere çalışmaya önem veririz:

1. Aras Digital bilgi varlıklarının bütünlük, erişilebilirlik ve gizlilik özelliklerinin gözetilmesi ve geliştirilmesi
2. Aras Digital BGYS Politikası 'na ve diğer BGYS kurallarına göre, şüpheli veya aykırı durumların, tüm çalışanların dikkati ve gözlemi altında olması ve söz konusu riskli durumların bildirilmesi
3. Aras Digital birimlerinin bilgi güvenliği risklerinin yönetilmesi, olası bilgi güvenliği olaylarına karşı önlemlerin tespiti, önlemlerin devreye alınması, sürdürülmesi, gözden geçirilmesi ve sürekli iyileştirmenin desteklenmesi