

Bak Ambalaj Bilgi Güvenliđi Politikası

Bak Ambalaj Bilgi Güvenliđi Yönetim Sistemi ařađıdaki temel prensiplere dayanmaktadır;

Güvenilirlik : Yetkilendirilmemiş kişiler, kuruluşlar veya başka işletim sistemlerinin bilgiye erişilebilirliğini veya ulaşılabilirliğini engellemek

Bütünlük : Varlıkların bütünlüğünü ve doğruluđunu korumak

Ulaşılabilirlik : Yetkilendirilmiş kişi talebi ile erişimi ve kullanılabilirliğini sağlamak

- ❖ İş stratejimiz, bilgi güvenliđi süreçleri ile ilgili güvenlik ihtiyaçları, riskler, zafiyetler ve fırsatları tanımlamak, değerlendirmek ve kontrolleri uygulamak için gerekli yönetim sistemini kurmak, geliřtirmek ve sürdürülebilirliğini ve sürekli iyileřtirilmesini sağlamak,
- ❖ Yasal, operasyonel ve sözleşme şartlarına tam uyum sağlayarak, fiziksel ve elektronik ortamda saklanan tüm bilginin gizlilik, bütünlük ve erişilebilirliğini sağlamak,
- ❖ Gümrük mevzuatı ile ilgili tüm yasal gerekliliklere tam uyumu sağlamak,
- ❖ Risklerin işlenmesi için çalışma esaslarını ortaya koymak, güvenlik risklerine yönelik kontrolleri geliřtirmek ve uygulamak. Teknolojik beklentileri ve geliřmeleri sürekli gözden geçirerek riskleri takip etmek,
- ❖ İş sürekliliđine yönelik bilgi güvenliđi risklerinin etkisini azaltmak ve iş sürekliliđini sağlamak,
- ❖ Gerçekleřebilecek bilgi güvenliđi olaylarına hızlı müdahale edebilecek ve olayın etkisini azaltacak yetkinliğe sahip olmak,
- ❖ Bilgi Güvenliđi risklerini en aza indirmek için, kullanıcıların ve çalışanların bilgi güvenliđi ile ilgili farkındalığını arttırmak, sorumluluklarının bilincine varmalarını sağlamak,
- ❖ Tanımlanmış hedefler ile bilgi güvenliđi performansını ve bilgi güvenliđi yönetim sisteminin etkinliğini değerlendirmek,
- ❖ Kişisel bilgilerin korunmasını sağlamak,
- ❖ Hizmet verilen elektronik altyapının güvenlik gereksinimlerini belirlemek, değerlendirmek, teknolojik geliřmeleri takip ederek geliřtirmek ve hizmet sürekliliđini sağlamak,
- ❖ Dış kaynaklı servis sağlayıcılarının bilgi güvenliđi sisteminin gerektirdiđi ihtiyaçlarını ve gereklilikleri yerine getirmesini sağlamak,
- ❖ Firma dışından sisteme erişimin sağlanması için kabul edilebilir güvenlik seviyesini sağlamak,
- ❖ 3.taraflar, müşteriler ve tedarikçilerin bilgi güvenliđi gereksinimlerini tanımlamak ve bilgi güvenliđi yönetim sistemine uymalarını sağlamak,
- ❖ Holding itibarını bilgi güvenliđi temelli olumsuz etkilerden korumak ve geliřtirmek,
- ❖ Grup şirketlerinin bilgi güvenliđi standartlarını belirlemek, düzenli aralıklarla denetlemek ve uygunluđu sağlamak.