BİLGİ GÜVENLİĞİ POLİTİKASI

1. AMAÇ

Tadım A.Ş. iş sürekliliğini sağlamak, bilgi güvenliği olay ve ihlalleri en aza indirmek ve etkilerini azaltmak, müşteriye, tedarikçiye ve çalışana ait olan bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlamak öncelikli amaçtır.

2. KAPSAM

Tüm Tadım A.Ş organizasyonunda uygulanmaktadır.

Tadım A.Ş; Gebze Organize Sanayi Bölgesi'nde bulunan Tadım Fabrika ve merkez depo ile Ataşehir İstanbul adresinde bulunan Tadım Pazarlama Ofisi, Kırıkkale ve Gaziantep'te bulunan üretim tesislerinden oluşmaktadır.

3. SORUMLULUK

Tadım A.Ş organizasyonunda yer alan tüm çalışanlar, Tadım' da uygulanan Bilgi Güvenliği faaliyetlerini yerine getirmek ve farkındalığın arttırılması amacıyla bu politikanın uygulanmasından sorumludur.

Üst Yönetim

Bilgi Güvenliği Politikası' nın kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

BG Yönetim Temsilcisi

Tadım A.Ş.' de Bilgi Güvenliği uygulamalarının etkin şekilde uygulanması ve yönetilmesine dek her aşamada üst yönetime karşı sorumluluk üstlenen BGYS temsilcisi bulunmaktadır.

BG Koordinasyon Ekibi

Üst yönetim tarafından görevlendirilen BG Koordinasyon Ekibi, Bilgi Güvenliği Politikasının kurum ihtiyaçlarını karşılar nitelikte bulunmasından, uygulanması için gerekli destek ve gözetimin sağlanmasından, politikanın en az yılda bir kez veya kurum politikasında değişiklik gerektirebilecek durumlarda gözden geçirilmesinden sorumludur.

Çalışanlar

Bilgi Güvenliği Politikasının gereklerinin görev alanlarının gerektirdiği biçimde yerine getirilmesinden sorumludur. Görev tanımlarında geçen bilgi güvenliği maddelerine uymaları ve QDMS üzerinden güncel bilgi güvenliği dokumanların takibinden sorumludur.

4. POLİTİKA

İnsan, altyapı, donanım, yazılım varlıkları, sözleşmeler ile belirlenen servis seviyelerine bağlı olarak yürütülen süreçlerin devamlılığı, şirket bilgileri, finansal kaynaklar ile ilgili her türlü

ortamda saklanan fiziksel ve elektronik bilgiler ile bulundukları ortamlar BG kuralları dahilinde korunur ve sistem sürekliliği takip edilir.

Fiziksel Sınırlar: Gebze Organize Sanayi Bölgesi'nde bulunan Tadım Fabrika ve merkez depo ile Ataşehir İstanbul adresinde Tadım Plaza'da 5~10. Katlar arasında Tadım Pazarlama Ofisi, Kırıkkale ve Gaziantep'te bulunan üretim tesisleri.

Sistem Sınırları: Tadım Fabrika ve Tadım Pazarlama ofisinde bulunan sunucu odaları, tüm Tadım lokasyonlarını bağlayan data hatları, UPS, Jeneratör gibi enerji kaynak cihazlarının bulunduğu alanlar, bilgisayar, notebook ve taşınabilir cihazlar (el terminallari,cep telefonu) , yazılımlar, işletim sistemleri ve tüm uygulamalar

Organizasyonel Sınırlar: Tadım Fabrika ve Pazarlama Ofis süreçleri kapsamında çalıştırdığı tüm personeli, 3. taraf ve yüklenicilerin hizmet veren personeli, lokasyondan bağımsız olarak hizmet veren teknik destek, bilgi teknolojileri, insan kaynakları, satın alma, kalite güvence personeli

Arayüzler: Tadım Fabrika, Tadım Pazarlama Ofisi, Kırıkkale ve Gaziantep üretim tesisleri güvenlik ana giriş ve çıkış noktaları, kart okuyucuları, fiziksel güvenlik uygulamaları, kamera sistemleri, kablosuz erişim noktaları, sunucu bağlantı noktaları

- 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 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 sektörel düzenlemelerden, yasal ve ilgili mevzuat gereklerini yerine getirmekten, anlaşmalardan doğan yükümlülüklerini karşılamaktan, iç ve dış paydaşlara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak.
- İş / hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmak
- Gerçekleşebilecek bilgi güvenliği olaylarına etkin ve hızlı müdahale edebilecek ve olayların etkilerini minimize edecek yetkinliğe sahip olmayı temin etmek.
- Maliyet etkin bir kontrol altyapısı ile bilgi güvenliği seviyesini zaman içinde korumak ve iyileştirmek.
- Kurumu ve itibarını bilgi güvenliği kırılmalarından kaynaklanabilecek olumsuz etkilerden korumak.
- Çalışanların bilgi güvenliğini farkındalığını geliştirmek.

Yönetim Desteği

- Üst yönetim, BG Koordinasyon Ekibi çatısı altında gerçekleştirdiği faaliyetler, BG İç Denetçi atamaları, BG yatırım, masraf ve eğitim bütçeleri, yönetim gözden geçirme aktiviteleri ile fiili olarak Bilgi Güvenliği faaliyetlerini destekler.

- Üst yönetim, BG politika ve prosedürlerine uyarak ve uyulmasını teşvik ederek BG hedeflerine ulaşmak için liderlik eder.

- Üst yönetim, bilgi güvenliği risklerinin yönetiminin kurumun itibarı ve faaliyetlerin sürekliliği açısından önemini yönetsel faaliyetleri uygulayarak ve kurumsal politikalar aracılığı ile ifade eder.

- Üst yönetim, yılda en az bir kez riskleri değerlendirir ve Bilgi Güvenliği Politikasını gözden geçirerek sistemin sürekliliğini, sürdürülebilirliğini temin eder.