GÜVENLİK POLİTİKASI

Bu politika, Midas A.Ş.'nin çalışanlarını, ürünlerini, tesislerini, bilgi varlıklarını ve tedarik zincirini güvenlik risklerine karşı korumak; yetkisiz erişim, hırsızlık, kaçakçılık, sabotaj, ürün manipülasyonu ve diğer güvenlik tehditlerini önlemek amacıyla oluşturulmuştur. Güvenlik, şirketimizin sürdürülebilir başarısı, çalışanların refahı, ürün ve tedarik zinciri bütünlüğü ile müşteri güveninin korunması açısından temel önceliklerimizdendir.

Bu politika; tüm çalışanları, ziyaretçileri, taşeronları, tedarikçileri, taşıyıcıları, lojistik hizmet sağlayıcılarını ve diğer ilgili iş ortaklarını kapsar. Şirket tesisleri, üretim alanları, depolar, ofisler, yükleme ve sevkiyat alanları, bilgi sistemleri ve şirket mülkleri politika kapsamındadır. Güvenlik uygulamalarında yürürlükteki mevzuatın yanı sıra uygulanabilir CTPAT MSC tedarik zinciri güvenliği kriterleri dikkate alınır.

1. **Çalışan Güvenliği**
   - Tüm çalışanlarımızın güvenliği önceliğimizdir.
   - İşyerinde şiddet, taciz ve ayrımcılığa sıfır tolerans uygulanır.
   - Acil durum tahliye planları hazırlanır, düzenli tatbikat yapılır.
   - İşe alım süreçlerinde pozisyonun risk seviyesine göre kimlik, özgeçmiş, referans ve gerekli yasal kontroller gerçekleştirilir.
   - İşten ayrılma veya görev değişikliği durumlarında fiziksel ve elektronik erişim yetkileri zamanında gözden geçirilir ve gerekli erişimler sonlandırılır/değiştirilir.

2. **Ürün Güvenliği**
   - Ürünlerin çalınmasını, hasar görmesini veya sahteciliğe uğramasını önlemek için gerekli tedbirler alınır.
   - Üretim ve depolama süreçlerinde güvenlik kontrolleri yapılır.
   - Sevkiyat öncesinde ürünler sayılır, kayıt altına alınır ve yetkisiz erişime karşı korunur.

3. **Bilgi ve Siber Güvenlik**
   - Şirketin bilgi sistemleri, ticari bilgileri, çalışan, müşteri, tedarikçi ve sevkiyat verileri yetkisiz erişim, kayıp, değiştirme ve kötüye kullanıma karşı korunur.
   - Bilgi sistemlerine erişimler görev ve yetki esasına göre sınırlandırılır.
   - Siber güvenlik tehditlerine karşı uygun teknik ve organizasyonel önlemler uygulanır.
   - Bilgi güvenliği ve siber güvenlik olayları kayıt altına alınır, değerlendirilir ve gerekli düzeltici faaliyetler uygulanır.

4. **Mülk ve Tesis Güvenliği**
   - Tesislere giriş-çıkışlar kontrol altında tutulur (kartlı geçiş, ziyaretçi kayıt sistemi vb.).
   - Kamera sistemleri ve alarm sistemleri ile tesis güvenliği sağlanır.

- Depolar, üretim alanları ve kritik bölgelere yetkisiz kişilerin girişi engellenir.
- Aydınlatma, çevre güvenliği, kamera, alarm, kilit ve erişim kontrol sistemlerinin etkinliği periyodik olarak kontrol edilir.
- Ziyaretçi, taşeron ve sürücülerin tesis içerisindeki erişimleri kontrol altında tutulur ve gerekli kayıtlar muhafaza edilir.

5. Tedarik Zinciri ve Sevkiyat Güvenliği

- Hammadde kabulünden nihai ürün sevkiyatına kadar ürün ve tedarik zinciri bütünlüğünün korunmasına yönelik güvenlik kontrolleri uygulanır.
- Taşıyıcılar, lojistik hizmet sağlayıcıları ve diğer kritik iş ortakları risk bazlı güvenlik kriterleri doğrultusunda değerlendirilir.
- Yükleme ve sevkiyat alanlarına erişim yetkilendirme esasına göre kontrol edilir.
- Sevkiyat araçları, konteynerler, paketler ve yüklerin bütünlüğünün korunmasına yönelik kontroller uygulanır.
- Gerekli sevkiyatlarda uygun yüksek güvenlikli mühürler kullanılır ve mühür kayıtları tutulur.
- Sevkiyat belgeleri ile ürün, miktar, paket ve gerekli durumlarda mühür bilgilerinin uyumu kontrol edilir.
- Şüpheli faaliyet, mühür bozulması, yük farklılığı, yetkisiz erişim veya diğer güvenlik olayları kayıt altına alınır, araştırılır ve gerekli aksiyonlar alınır.

6. Uygulama ve Sorumluluklar

- Bu politikanın uygulanması için gerekli prosedürler hazırlanır ve düzenli olarak gözden geçirilir.
- Tüm çalışanlar, bu politikaya uygun hareket etmekle yükümlüdür.
  Güvenlik ihlalleri, şüpheli faaliyetler ve güvenlik olayları derhal ilgili yöneticilere bildirilir, kayıt altına alınır ve gerekli durumlarda araştırılarak düzeltici/iyileştirici faaliyet başlatılır. İlgili mevzuat veya olayın niteliği gerektirdiğinde yetkili kamu kurumları ve ilgili taraflarla iletişim sağlanır.

7. Sürekli İyileştirme

- Güvenlik uygulamaları düzenli olarak denetlenir.
- Çalışanlardan gelen geri bildirimler dikkate alınır.
- Yeni riskler ve teknolojiler doğrultusunda politika güncellenir.

Yönetim Kurulu Adına
Bülent ÖZKÖK
10.08.2026

8. YAŞAM FİŞİ

Revizyon No	Revizyon Tarihi	Açıklama
0	**25.08.2025**	**İLK YAYIN**
1	**10.08.2026**	**Yıllık gözden geçirme gerçekleştirilmiştir.**