SUNUCU GÜVENLİK POLİTİKASI

1.0 AMAÇ

Bu politikanın amacı ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in sahip olduğu sunucularının temel güvenlik yapılandırması için standartları belirlemektir. Bu politikanın etkili kullanılması ile ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in bünyesindeki bilgilere ve teknolojiye yetkisiz erişimler minimize edilecektir.

2.0 KAPSAM

Bu politika ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in sahip olduğu bütün dâhili sunucuları kapsamaktadır.

3.0 POLİTİKA

3.1. Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dâhili sunucuların yönetiminden sadece yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.

a) Bütün sunucular (kurumun sahip olduğu) ilgili kurumun yönetim sistemine kayıt olmalı ve en az aşağıdaki bilgileri içermelidir.

- Sunucuların yeri ve sorumlu kişi
- Donanım ve işletim sistemi
- Ana görevi ve üzerinde çalışan uygulamalar
- İşletim sistemi sürümleri ve yamalar

b) Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

3.2. Genel Konfigurasyon Kuralları

a) İşletim sistemi konfigurasyonları kurumun bilgi işlem biriminin talimatlarına göre yapılacaktır.

b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.

c) Active directory de 1 hafta süreyle loglanacaktır. (IP bazlı)

d) Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (IPSEC, SSL,VPN) üzerinden yapılmalıdır.

e) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.

3.3. Gözlemleme

a) Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalı ve aşağıdaki şekilde saklanmalıdır.

- Active directory IP bazlı olarak bir hafta süreyle erişilebilmelidir.
- Önem derecesine göre exchange veritabanı haftalık, müşteri kaynak kodları haftalık, tüm kaynak kodları database günlük, iletşim sistemleri günlük alınır ve 15 gün saklanır.
- Aylık full backuplar en az 1 yıl tutulmalıdır.

b) Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikle ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.

- Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

3.4. Uygunluk

- Denetimler yetkili organizasyonlar tarafından kurum bünyesinde belli aralıklarda yapılmalıdır.

- Denetimlerde kurumun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

3.5. İşletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
- Sunucuların yazılım ve donanım bakımları 2 aylık sürelerde, sistem yöneticileri tarafından yapılmalıdır.
- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı.