KABLOSUZ İLETİŞİM POLİTİKASI

1.0 AMAÇ

Bu politikanın amacı, kablosuz cihazların gerekli güvenlik tedbirleri alınmaksızın ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ 'in ait bilgisayar ağına erişiminin engellenmesi hakkında kuralları belirlemektir.

Sadece bu politikanın güvenlik kriterlerine uyan cihazlar kurumun bünyesinde kullanabilirler.

2.0 KAPSAM

Bu politika ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarını kapsamaktadır. Kablosuz veri transferi sağlayabilen herhangi bir cihaz bu politikanın kapsamındadır. Kurumla bağlantısı olmayan herhangi bir cihaz veya bilgisayar ağı bu politikanın kapsamı içerisinde değildir.

3.0 POLİTİKA

3.1. Onaylanmış Teknoloji

Bütün kablosuz erişim cihazları yetkili birim tarafından onaylanmış olmalıdır ve belirlenen güvenlik ayarlarını kullanmalıdır.

3.2. Güvenlik Ayarları

a) Güçlü bir şifreleme ve erişim kontrol sistemi kullanılmalıdır. Bunun için Wi-Fi Protected Access şifreleme kullanılmalıdır.

b) Erişim cihazlarındaki firmware ları düzenli olarak güncellenmelidir. Bu, donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

c)Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.

d) Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.

e) Varsayılan SSID isimlerini kullanmayınız. SSID bilgisi içerisinde kurumla ilgili bilgi olmamalıdır. Mesela kurum ismi, ilgili bölüm çalışanın ismi vs.

f) Erişim cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.

g) Kullanıcı bilgisayarlarında kişisel firewall yazılımları yüklü olmalıdır.

h) Kritik yerlerde kullanıcılar VPN teknolojilerini kullanarak kurum ağına erişmelidirler.

j) Hem kullanıcılar hem de erişim cihazları statik ip adresleri kullanmalıdır. Aynı zamanda donanım adresleme kullanılmalıdır.

k) Erişim cihazlarını bir yönetim yazılımı ile devamlı olarak gözlemlenmelidir. Sistemde hackerlar tarafından konulmuş casus bir erşim cihazı olabilir veya mevcut erişim cihazı resetlenmiş olup kurumun güvenlik politikalarına aykırı bir şekilde ayar yapılmış olabilir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		