UZAKTAN ERİŞİM POLİTİKASI

1.0 AMAÇ

Bu politikanın amacı herhangi bir yerden kurumun bilgisayar ağına erişilmesine ilişkin standartları saptamaktır. Bu standartlar kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları minimize etmek için tasarlanmıştır. Bu zararlar şunlardır, ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in gizli ve hassas bilgilerin kaybı, itibar kaybı ve içerideki kritik sistemlerde meydana gelen zararlar vs.

2.0 KAPSAM

Bu politika ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in bütün çalışanlarını, sözleşmelileri veya kurum adına çalışanları ve kısaca kurumun herhangi bir birimindeki bilgisayar ağına erişen bütün kişi ve kurumları kapsamaktadır.

Bu politika, kuruma bağlı bütün uzak erişim bağlantılarını kapsamaktadır ve bunun içerisine e-posta okuma veya gönderme ve intranet web kaynaklarını gözlemleme dâhildir. Bütün uzaktan erişim uygulamaları bu politika tarafından kapsanmaktadır. Modemden port yönlendirmesi (RDP) , VPN ile sınırlıdır.

3.0 POLİTİKA

3.1. Genel

a) Uzaktan erişim için yetkilendirilmiş kurum çalışanları veya kurumun bilgisya ağına bağlanan diğer kullanıcılar yerel ağdan bağlanan kullanıcılar ile eşit sorumluluğa sahiptir.

b) Uzaktan erişim metotları ile kuruma bağlantılarda bilgi sistemlerinin güvenliğinin sağlanması için aşağıdaki politikalara göz atmak gerekmektedir.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

- Kabul edilebilir şifreleme politikası
- Sanal Özel Ağ (VPN) Politikası

3.2 Gereklilikler

a) İnternet üzerinden kurumun herhangi bir yerindeki bilgisayar ağına erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır. Bu; veri bütünlüğünün korunması, erişim denetimi, mahremiyet, giziliğin korunması ve sistem devamlılığını sağlayacaktır. VPN teknolojileri IpSec, L2TP, SSL, PPTP vs.protokollerinden birini içermelidir.

b) Mümkünse uzaktan erişim güvenliği sıkı bir şekilde denetlenmelidir. Kontrol tek yönlü şifreleme (one time password authentication) veya güçlü bir passpharase (uzun şifre) destekli public /private key sistemi kullanılması tavsiye edilmektedir. Daha fazla bilgi için şifreleme bölüme bakınız.

c) Kurum çalışanları hiçbir şekilde kendilerinin login ve e-posta şifrelerini aile bireyleri dâhil olmak üzere hiç kimseye veremezler.

d) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar. Kullanıcının tamamıyla kontrolünde olan ağlarda bu kural geçerli değildir.

e) Çalışanlar kurum ile ilgili çalışmalarında kurumun dışındaki e-posta hesaplarını kullanamazlar.

g) Uzaktaki kullanıcı cihazını split-tunnel veya dual homing (VPN bağlantısı esnasında başka bir bağlantı daha yapmak) olarak konfigure edemez.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

i) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler birimin özel izni ile geçici olarak izin verilebilirler.

j) Periyodik olarak yapılan kontrollerle kurumdan ilişiği kesilmiş veya görevi değişmiş kullanıcı kimilikleri ve hesapları kaldırılmalıdır.

	HAZIRLAYAN	ONAYLAYAN
ÜNVAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		