	BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKALARI	Yayın Tarihi	15.11.2019
		Revizyon Tarihi	-
		Revizyon No	00
FİRMALAR İÇİN UZAKTAN ERİŞİM POLİTİKASI			

1.0 AMAÇ

Bu politikanın amacı, firmaların herhangi bir yerden ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ'in bilgi sistemlerine erişmesine ilişkin normları belirlemektir.


2.0 KAPSAM

Bu politika, ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ'e uzaktan hizmet veren kişi veya kurumları kapsamaktadır.

3.0 POLİTİKA

- Kurum ve firma arasında şifreli iletişim hatları kullanılacaktır; internet üzerinden kurumun herhangi bir yerindeki bilgisayara erişen kişi veya kurumlar VPN teknolojisini kullanacaklardır.
- Uzaktan erişilen yer mutlaka statik IP ye sahip olmalı ve bu IP kurumun güvenlik cihazlarında tanımlanmış olmalıdır.
- Firma uzaktankimlerin hangi rollerde kurum bilgisayarlarına eriştiğini belirtecek ve ayrıca ilgili kişilerin bilgisayarlara erişimde kullandığı kullanıcı adı ve şifreleri kurumdaki en üst yetkiliye teslim edecektir.
- Kullanıcıların erişim şifrelerini az 4 ayda bir değiştirilecektir. Verilen şifreler kurumun şifreleme politikasına uygun olacaktır.
- Firma, kurumun hiçbir bilgisini görüntüleyemez, ekran çıktısını alamaz, transfer edemez ve kurum dışına çıkartamaz. Aksi takdirde oluşacak yasal yükümlülüklerden firma sorumlu olacaktır.
- Uzaktan erişim için mümkünse tek yönlü şifreleme veya güçlü bir uzun şifre destekli public/private key sistemi kullanılması tavsiye edilmektedir.

	HAZIRLAYAN	ONAYLAYAN
ÜN VAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

	BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKALARI	Yayın Tarihi	15.11.2019
		Revizyon Tarihi	-
		Revizyon No	00
FİRMALAR İÇİN UZAKTAN ERİŞİM POLİTİKASI			

- g) Firma çalışanları hiçbir şekilde kendilerinin login şifrelerini aile bireyleri dahil olmak üzere hiç kimseye veremezler
- h) Kurumun ağına uzaktan bağlantı yetkisi verilen çalışanlar bağlantı esnasında aynı anda başka bir ağa bağlı olmadıklarından emin olmalıdırlar.
- i) Uzaktan bağlanan kişi makinasında zararlı kod, truva atı, vs. olduğundan şüpheleniyorsa bağlantıyı gerçekleştirmemlidir.
- j) Uzaktan erişim yöntemi ile kuruma erişen bilgisayar ağında güvenlik tedbirleri alınmış olmalıdır.(örn, firewall, Domain altyapısı vs.)
- k) Kurum ağına standart dışı erişim isteğinde bulunan organizasyon veya kişiler kurumun bilgi işlem biriminden izin almak zorundadırlar.
- l) Firma, periyodik olarak kullanıcı kimlikleri ve hesapları kontrol etmeli gereksiz kullanıcı kimlikleri ve hesapları kaldırılmalıdır.
- m) Firma, kurum ile hassas veriye erişim hakkında gizlilik anlaşması imzalamalıdır.
- n) Kurum, firmanın alması gereken güvenlik tedbirlerinde herhangi bir aksaklık gördüğünde kurum ve firma arasındaki uzaktan erişim bağlantısını eksiklik düzeltilinceye kadar kesebilir.
- o) Kurum güvenli erişimin sağlanabilmesi için gerekli gördüğü takdirde firmanın sadece belli zaman aralıklarında veya istek yapılan durumda uzaktan erişimine izin verebilir.

	HAZIRLAYAN	ONAYLAYAN
ÜN VAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		