

	<b>BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKALARI</b>	Yayın Tarihi	15.11.2019
		Revizyon Tarihi	-
		Revizyon No	00
<b>PERSONEL GÜVENLİĞİ POLİTİKASI</b>			

## 1.0 AMAÇ

ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in bilgi kaynaklarının güvenliğinin sağlanması, çalışanlarının bu konuya duyarlı olması, bilinç seviyesi kendisine verilen yetki ve sorumlulukları iyi anlaması ve yerine getirmesiyle çok yakından bağlantılıdır. Bu nedenle ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in ilgili personelin seçimi sorumluluk ve yetkilerin atanması, işten atılması, eğitilmesi vb.konularının güvenlik ile ilgili boyutunu ne şekilde ele alacağını bu politika ile belirler.

## 2.0 KAPSAM

Bu politika ÜNAL GIDA VE İNŞ. SAN. TİC. LTD. ŞTİ in bilgi sistemlerini kullanan tüm yönetici ve çalışanlarını kapsamaktadır.

## 3.0 POLİTİKA

- Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
- Kullanıcılara erişim haklarını açıklayan yazılı bildirimler verilmeli ve teyit alınmalıdır.
- Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.
- Bilgi sistemlerinde sorumluluk verilecek kişinin özgeçmişi araştırılmalı, beyan edilen akademik ve profesyonel bilgiler teyit edilmeli, karakter özellikleriyle ilgili tatmin edici düzeyde bilgi sahibi olmak için iş çevresinden ve dışından referans sorulması sağlanmalıdır.
- Bilgi sistemleri ihalelerinde sorumluluk alacak firma personeli için güvenlik gereksinim ve incelemeleriyle ilgili koşullar eklenmelidir.
- Kritik bilgiye erişim hakkı olan çalışanlar ile gizlilik anlaşmaları imzalanmalıdır.
- Kurumsal bilgi güvenliği bilinçlendirme eğitimleri düzenlenmelidir.

	HAZIRLAYAN	ONAYLAYAN
ÜN VAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		

	<b>BİLGİ GÜVENLİĞİ YÖNETİM POLİTİKALARI</b>	Yayın Tarihi	15.11.2019
		Revizyon Tarihi	-
		Revizyon No	00
<b>PERSONEL GÜVENLİĞİ POLİTİKASI</b>			

- h) Çalışanlara telefon görüşmeleri yaparken civardakiler tarafından işitilebileceği veya dinlenebileceği için hassas bilgilerin konuşulmaması hatırlatılmalıdır.
- i) Çalışanlara kamuya açık alanlarda, açık ofis ortamlarında ve ince duvarları olan odalarda gizliliği olan konuşmaların yapılmaması hatırlatılmalıdır.
- j) İş tanımı değişen veya kurumdan ayrılan kullanıcıların erişim hakları hemen silinmelidir.
- k) Kurum bilgi sistemlerinin işletilmesinden sorumlu personelin konularıyla ilgili teknik bilgi düzeylerini güncel tutmaları çalışma sürekliliği açısından önemli olduğundan eğitim planlamaları periyodik olarak yapılmalı, bütçe ayrılmalı eğitimlere katılım sağlanmalı ve eğitim etkinliği değerlendirilmiştir.
- l) Yetkiler “görevler ayrımı” ve “en az ayrıcalık” esaslı olmalıdır. “Görevler ayrımı “ rollerin sorumlulukların paylaşılması ile ilgilidir ve bu paylaşım sayesinde kritik bir sürecin tek kişi tarafından kırılma olasılığı azaltılır.”En az ayrıcalık” ise kullanıcıların gereğinden fazla yetkiyle donatılmamaları ve sorumlu oldukları işleri yapabilmeleri için yeterli olan asgari erişim yetkisine sahip olmaları demektir.
- m) Kritik bir görevin tek kişiye bağımlılığını azaltmak ve aynı işi daha fazla sayıda çalışanın yürütebilmesini sağlamak amacıyla, bir sıra dâhilinde çalışanlara görev ve sorumluluk atanmalıdır. Böylece kritik bir iş birden fazla kişi tarafından öğrenilmiş olacaktır.
- n) Çalışanlar kendi işleri ile ilgili olarak bilgi güvenliği sorumlulukları, riskler görev ve yetkileri hakkında periyodik olarak eğitilmelidir. Yeni işe alınan elemanlar içinde bu eğitim, oryantasyon sırasında verilmelidir.

	HAZIRLAYAN	ONAYLAYAN
ÜN VAN	YÖNETİM TEMSİLCİSİ	GENEL MÜDÜR
İMZA		