

## TUVEO KURUMSAL GAYRİMENKUL DEĞERLEME VE DANIŞMANLIK A.Ş. 2016 YILINA AİT KALİTE GÜVENCE SİSTEMİ GÖZDEN GEÇİRME RAPORU

2005 yılından beri değerlendirme sektöründe faaliyet göstermiş ve çalışmaları ile tanınan TUVEO Gayrimenkul Değerleme Limited Şirketi, değerlendirme sektöründe uzun yıllar hizmet vermiş ve SPK Lisansına sahip Değerleme Uzmanları ile gücünü birleştirerek 27.01.2011 tarihinde İZMİR merkezli olarak TUVEO KURUMSAL GAYRİMENKUL DEĞERLEME VE DANIŞMANLIK ANONİM ŞİRKET 'ine dönüşmüştür.

### Şirketimiz;

- Sermaye Piyasası Kurulu tarafından ( SPK ) yayınlanan, değerlendirme şirketlerinin kurulca listeye alınma esasları tebliği kapsamındaki şartları sağlayarak, 29 Nisan 2011 tarihi itibarıyla, Sermaye Piyasası Kurulu tarafından değerlendirme hizmeti verecek şirketler listesine alınmıştır.
- Bankacılık Düzenleme ve Denetleme Kurumunca hazırlanan 1 Kasım 2006 tarih ve 26333 sayılı resmi gazetede yayınlanan, bankalara değerlendirme hizmeti verecek kuruluşların yetkilendirilmesi ve faaliyetleri hakkındaki yönetmelik ile 29 Eylül 2007 tarih ve 26658 sayılı resmi gazetede yayınlanan, bankalara değerlendirme hizmeti verecek kuruluşların yetkilendirilmesi ve faaliyetleri hakkındaki yönetmelikte değişiklik yapılmasına ilişkin yönetmeliğin 11. Maddesine istinaden bankalara yönetmeliğin 4. maddesi kapsamına giren değerlendirme faaliyetlerinden “gayrimenkul, gayrimenkul projesi veya bir gayrimenkule bağlı hak ve faydaların değerlendirilmesi” hizmeti verme konusunda yetkilendirilmiş ve Bankacılık Düzenleme ve Denetleme Kurumu ( BDDK ) tarafından 02.11.2011 tarih 4446 sayılı kurul kararı ile bankalara değerlendirme hizmetleri verecek kuruluşların yetkilendirilmesi ve faaliyetleri hakkındaki yönetmeliğin 4. Maddesi kapsamına göre **“gayrimenkul, gayrimenkul projesi veya gayrimenkule bağlı hak ve faydaların değerlemesi”** hizmeti verecek şirketler listesine alınmıştır.
- BDDK'nın 01.10.2006 tarih, 26333 sayılı Bankalara Değerleme Hizmeti Verecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmeliğin 15 Maddesindeki hususları da gözetilerek ZÜRİH Sigorta Firmasına 3.000.000.-TL üzerinden Mesleki Sorumluluk Sigortası yaptırmıştır.

İş bu rapor, Bankacılık Düzenleme ve Denetleme Kurumu tarafından 1 Kasım 2006 Tarih ve 26333 Sayılı Resmi Gazetede yayımlanan Bankalara Değerleme Hizmeti Verecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmeliğin 8. maddesi uyarınca ve ilgili maddenin 4. fıkrası uyarınca Tuveo Kurumsal Gayrimenkul Değerleme ve Danışmanlık A.Ş'nin kalite güvence sistemi işleyişinden sorumlu Yönetim Kurulu Üyesi Zuhal ÇERÇİ tarafından hazırlanıp Yönetim Kurulu tarafından onaylanmıştır.

İlgili maddenin “kalite güvence sistemi yılda bir kez gözden geçirilir ve gözden geçirmenin kapsamı, değerlendirme kuruluşunun internet sitesinden kamuoyuna yayımlanır” fıkrası uyarınca internet sitemizden kamuoyuna açıklanmıştır.

Saygılarımla,

Zuhal ÇERÇİ

**Kalite Güvence Sisteminin İşleyişinden Sorumlu**

**Yönetim Kurulu Üyesi**

## İÇİNDEKİLER

1. GENEL BİLGİ.....	3
2. TUVEO KURUMSAL DEĞERLEME 25.10.2013 TARİHİ İTİBARI İLE ŞİRKET ORTAKLIK YAPISI-YÖNETİM KURULU- LİSANSLI DEĞERLEME UZMANLARI .....	3
3. PERSONEL YAPISI.....	4
3.1 DEĞERLEME İLE İŞTİGAL EDEN KADROLU PERSONEL YAPISI .....	4
3.2 KALİTE GÜVENCE SİSTEMİ PERSONEL YAPISI .....	4
3.3 İDARİ PERSONEL YAPISI.....	4
3.4 ŞİRKET DANIŞMANLARI.....	5
4. HİZMET VERİLEN BANKALAR, KURUMLAR VE SEKTÖRLER.....	5
4.1 Çalışılan Bankalar .....	5
4.2 Çalışılan Kurumlar .....	5
4.3 Özel Sektör .....	6
5. KALİTE GÜVENCE SİSTEMİNİN GENEL YAPISI VE GÖZDEN GEÇİRİLMESİNE İLİŞKİN DEĞERLENDİRME.....	7
5.1 Kalite Güvence Sisteminin Genel Yapısı.....	7
5.2 Kalite Güvence Sisteminin Temel Etik İlkeleri.....	7
5.3 Kalite Güvence Sisteminin Gözden Geçirilmesine İlişkin Değerlendirme .....	7
5.4 TUVEO KALİTE POLİTİKASI.....	9
6. KALİTE GÜVENCE SİSTEMİNE EK OLARAK GELİŞTİRİLEN BİLGİ GÜVENLİĞİ POLİTİKASI.....	9
6.1 BİLGİ GÜVENLİĞİ HAKKINDA 2012/3 NOLU TEBLİĞ İÇERİĞİ VE MADDELERİ .....	9
7. KALİTE GÜVENCE SİSTEMİNİN İŞLEYİŞİNDEN SORUMLU YÖNETİM KURULU ÜYESİNE İLİŞKİN BİLGİLER;.....	16


## 1. GENEL BİLGİ

Firmamız TUVEO Kurumsal Gayrimenkul Değerleme ve Danışmanlık A.Ş. bağımsız olarak Sermaye Piyasası Kurulu yetkilendirmesi ve Bankacılık Düzenleme ve Denetleme Kurumu'nun listesinde ve Bankacılık Düzenleme ve Denetleme Kurumu'nun denetiminde uluslararası standartlarda değerlendirme (ekspertizlik) hizmetleri vermeye yetkilendirilmiş bir kuruluştur.

Firmamız, ISO 9001:2008 Kalite Yönetim Sistemi standartlarına uygun olup ayrıca verilen hizmetin her aşamasındaki sorumlulukları SPK ve BDDK tarafından tanımlanmıştır.

Uluslararası standartlardaki Bağımsızlık, Sorumluluk, Mesleki özen ve Titizlik ve Sır saklama yükümlülüğü ilkeleri doğrultusunda çalışırken faaliyetlerimizden ya da mesleki hatalardan doğabilecek zararlar için, BDDK tarafından ana hatları belirlenen Mesleki Sorumluluk Sigortası 3 milyon TL üzerinden yaptırılmıştır.

## 2. TUVEO KURUMSAL DEĞERLEME 31.12.2016 TARİHİ İTİBARI İLE ŞİRKET ORTAKLIK YAPISI-YÖNETİM KURULU-LİSANSLI DEĞERLEME UZMANLARI

 TUVEO KURUMSAL GAYRİMENKUL DEĞERLEME VE DANIŞMANLIK A.Ş.			
ORTAKLIK YAPISI			
ADI SOYADI VE YA TİCARET ÜNVANI	SORUMLU ORTAK OLUP/OLMADIĞI	PAY TUTARI ÖDENMİŞ (TL)	PAY ORANI ÖDENMİŞ (%)
SEBATİ ALTUN	SORUMLU ORTAK	86,800	31
MİRAY TUĞÇE ÇERÇİ	SORUMLU ORTAK	91,000	32,5
ZUHAL ÇERÇİ	-	53,200	19
OĞUZHAN ÇERÇİ	-	49,000	17,5
YÖNETİM KURULU ÜYELERİ, GENEL MÜDÜR, GENEL MÜDÜR YARDIMCISI VE DENETÇİ			
ADI SOYADI	ÜNVANI		
MİRAY TUĞÇE ÇERÇİ	Yönetim Kurulu Başkanı		
ZUHAL ÇERÇİ	Yönetim Kurulu Başkan Yardımcısı		
SEBATİ ALTUN	Yönetim Kurulu Üyesi		
OLGU BAĞIMSIZ DENETİM VE YEMİNLİ MALİ MÜŞAVİRLİK A.Ş.	DENETÇİ		
ADI SOYADI	LİSANS BELGESİ TARİHİ VE NUMARASI	İŞ TECRÜBESİ	
SEBATİ ALTUN	27.02.2006 / 400301	Sorumlu Değerleme Uzmanı	
MİRAY TUĞÇE ÇERÇİ	26.01.2012 / 401886	Sorumlu Değerleme Uzmanı	
KUDRET ERGÜN	28.11.2008 / 400898	Lisanslı Değerleme Uzmanı	
EREN ORHAN	17.06.2014 / 402843	Lisanslı Değerleme Uzmanı	
TEVFİDE YAŞAR	25.12.2014 / 403097	Lisanslı Değerleme Uzmanı	
ALTUĞ AKPINAR	29.08.2014 / 403078	Lisanslı Değerleme Uzmanı	

### 3. PERSONEL YAPISI

#### 3.1 DEĞERLEME İLE İŞTİĞAL EDEN KADROLU PERSONEL YAPISI

ADI SOYADI	MESLEK
SEBATİ ALTUN	Sorumlu Değerleme Uzmanı
MİRAY TUĞÇE ÇERÇİ	Sorumlu Değerleme Uzmanı
KUDRET ERGÜN	Değerleme Uzmanı
EREN ORHAN	Değerleme Uzmanı
ALTUĞ AKPINAR	Değerleme Uzmanı
TEVFİDE ÖZGÜN	Değerleme Uzmanı
TANER TİRYAKİ	Değ. Uzm. Yrd.
GÖKHAN SEMERCİ	Değ. Uzm. Yrd.
ÖZGÜR YENİL	Değ. Uzm. Yrd.
GÜL BAHAR ŞEKER	Değ. Uzm. Yrd.
ERDEM YILDIRIM	Değ. Uzm. Yrd.
ESRA GÖKDEMİR	Değ. Uzm. Yrd.
MURAT KATITAŞ	Değ. Uzm. Yrd.
OĞUZHAN ÇERÇİ	Değ. Uzm. Yrd.

#### 3.2 KALİTE GÜVENCE SİSTEMİ PERSONEL YAPISI

Adı Soyadı	Mesleki Unvanı	Şirketteki Unvanı	Şirketteki Görevinin Kapsamı
Zuhal Çerçi	Ziraat Mühendisi	Yönetim Kurulu Üyesi	Kalite birimi sorumlusu ve Uygulayıcısı

#### 3.3 İDARİ PERSONEL YAPISI

Adı Soyadı	Şirketteki Unvanı	Şirketteki Görevinin Kapsamı
TÜRKAN AKÇAY	Muhasebe-İK ve Finans Sorumlusu	Muhasebe - Personel işleri
BURÇİN GENÇ	Operasyon Sorumlusu	Talep Giriş ve Süreç takip
PELİN AKCALI EKİNCİ	Operasyon Sorumlusu	Talep Giriş ve Süreç takip
PINAR SATU	Operasyon Sorumlusu	Talep Giriş ve Süreç takip
BAŞAK AYAR	Operasyon Sorumlusu	Talep Giriş ve Süreç takip
HAVA KELEŞ	Yardımcı personel	Ofis Hizmetleri

### 3.4 ŞİRKET DANIŞMANLARI

Adı Soyadı	Mesleki Unvanı	Şirketteki Unvanı
FİLİZ AVCI FALAY	AVUKAT	ŞİRKET SÖZLEŞMELİ AVUKATI
ALİ GENÇ	AVUKAT	HUKUK DANIŞMANI SPK LİSANSLI DEĞERLEME UZMANI
AHMET DİKER	GAZETECİ	BASIN DANIŞMANI
ZERRİN HASDEMİR-İZTİM	NETSİS YAZILIMCISI	WEB SİTESİ DANIŞMANI
UMUT ALTINGÖZ	YAZILIM GELİŞTİRME UZM.	YAZILIM DANIŞMANI ( İŞ YAZILIM)
LEVENT ACAR-EOFİSİM	MAKİNE MÜHENDİSİ	BİLGİ GÜVENLİĞİ DANIŞMANI
ZUHAL ÇERÇİ	ZİRAAT MÜHENDİSİ	TARIM DANIŞMANI
OKTAY KUZUĞ	MAKİNE MÜHENDİSİ	MAKİNE DANIŞMANI

## 4. HİZMET VERİLEN BANKALAR, KURUMLAR VE SEKTÖRLER

### 4.1 Çalışılan Bankalar

Türkiye İş Bankası A.Ş.

Akbank T.A.Ş.

Denizbank A.Ş.

T. Halk Bankası A.Ş.

Anadolu Bank A.Ş.

### 4.2 Çalışılan Kurumlar

Tasarruf Mevduatı ve Sigorta Fonu

Akleasing

Denizleasing

İzmir Foça Belediyesi

Çanakkale Geyikli Belediyesi

### 4.3 Özel Sektör

Egezemin A.Ş.

Lodos Basınçlı Döküm Ltd. Şti.

Saraçoğlu Tekstil

Batıçim Çimento

Yonca Gıda

Balatacılar Balatacılık San. Tic. A.Ş.

Kavuklar Akaryakıt A.Ş.

Aybak Natura Analiz

Meba Kağıt

Burda Marketçilik

Suntopia Otel

Dalan Kimya

Tariş

Atar Mobilya

Kale Bayar İnşaat

Ulusoy Su Pompaları

Hisar İnşaat

Şahin Granit

Cem Dağ Aydınlatma

Vindo

Batıçim

Geyikli Belediye Başkanlığı

Cemdağ Aydınlatma ve Tic. A.Ş.

Şahıs talepleri



## 5. KALİTE GÜVENCE SİSTEMİNİN GENEL YAPISI VE GÖZDEN GEÇİRİLMESİNE İLİŞKİN DEĞERLENDİRME

### 5.1 Kalite Güvence Sisteminin Genel Yapısı

- Şirket Yönetim Kurulunca Ziraat Mühendisi Zuhal ÇERÇİ Kalite Güvence Sisteminin işleyişinden sorumlu yönetim kurulu üyesi olarak görevlendirilmiştir. Şirket tarafından sunulan hizmetlerin kalitesini sürekli kılmak amacıyla Kalite Yönetim Sistemi oluşturulmuştur. Yapılan denetimler sonucunda Şirketimiz, 24 Ocak 2013 tarihinde **Türk Standartları Enstitüsü** tarafından ISO 9001:2008 Kalite Yönetim Sistemi ile sertifikalandırılmıştır ve bu sertifika uyarınca kalite sistemi standartlarını yerine getirmekte ve uygulamaktadır.

Bankacılık Düzenleme ve Denetleme Kurumu tarafından 1 Kasım 2006 Tarih ve 26333 Sayılı Resmi Gazetede yayımlanan Bankalara Değerleme Hizmeti Verecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmeliğin 8.maddesi 5.fıkrasına göre kalite güvence sisteminin aşağıda belirtilen ilkelerine uygun yürütülmektedir.

- **MESLEKİ GEREKLİLİKLER:** Değerleme kuruluşunun değerlendirme faaliyeti ile işgal eden personelinin Bankalara Değerleme Hizmeti Verecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik'in 5, 6, 7, 9, 10 ve 20. madde hükümlerine uygun davranması.
- **MESLEKİ YETERLİLİK:** Değerleme kuruluşunun değerlendirme faaliyeti ile işgal eden personelinin, sorumluluklarını doğru bir şekilde yerine getirebilmesi için gerekli bilgi ve yeterliliğe sahip olması.
- **GÖREV DAĞILIMI:** Değerleme çalışmasının gerekli düzeyde bilgi, mesleki yeterlilik ve beceriye sahip olan kişiler tarafından gerçekleştirilmesi.
- **YÖNLENDİRME:** Değerleme faaliyetinin istenen kalitede olabilmesini ve değerlendirme sonunda tam ve doğru bir görüş bildirilebilmesini teminen, yapılan işin her seviyede gözden geçirilmesi ve değerlendirme ile görevlendirilen personelin görevleri konusunda yönlendirilmesi.
- **GÖRÜŞ ALMA:** Gerekli görülen durumlarda, konuyla ilgili deneyimi ve bilgisi bulunan kişilerden görüş alınması.
- **GÖREV KABULÜ VE DEVAMLILIK:** Yeni görev kabulü için veya gelecek dönemlerde değerlendirme faaliyetine devam edilebilmesi için değerlendirme yapılması, yapılacak değerlendirmede bankanın durumunun özellikle bağımsızlık ilkelerine uygunluk ve verilecek hizmetin kapsam ve boyutu yönünden değerlendirilmesi.
- **İZLEME:** Kalite güvence sisteminin ve işlevselliğinin izlenmesi.

### 5.2 Kalite Güvence Sisteminin Temel Etik İlkeleri

Kalite Güvence Sisteminden Sorumlu Yönetim Kurulu Üyesi Zuhal ÇERÇİ tarafından değerlendirme uzmanları ve diğer personele temel etik ilkeler olan Bağımsızlık, Dürüstlük, Tarafsızlık, Mesleki Yeterlilik, Mesleki Özen ve Titizlik, Sır Saklama hususlarının uygulanması konusunda önceden yapılmış olan eğitimler tekrarlanmış olup eski ve yeni personele kalite güvence sistemimiz ile ilgili gerekli açıklamalar yapılmıştır.

### 5.3 Kalite Güvence Sisteminin Gözden Geçirilmesine İlişkin Değerlendirme

- Şirket bünyesinde yer alan ve Değerleme faaliyeti içerisinde aktif rol alan personelin, görevlerini; dürüstlük, doğruluk, gizlilik, tarafsızlık ve bağımsızlık ilkelerine bağlı olarak, çıkar ilişkilerinden uzak, tarafsızlıklarını etkileyecek hiçbir müdahaleye izin vermeden tam bir bağımsızlık içinde yürüttükleri, Bankalara Değerleme Hizmeti Verecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik'in 5, 6, 7, 9, 10 ve 20 . Madde hükümlerine uygun davranıldığı,

- Bu hizmetleri yürüten personelin sorumluluklarını doğru bir şekilde yerine getirebilmeleri için Yönetmeliğin 3.madde (ı) fıkrasında belirtilen “değerleme faaliyeti ile iştigal eden personel” (Değerleme faaliyeti ile iştigal eden personel: Değerleme kuruluşu tarafından değerlendirme yapmak üzere istihdam edilen, en az dört yıllık lisans düzeyinde öğrenim görmüş, bankacılık, bağımsız denetim veya mahkemelerde bilirkişilik de dahil olmak üzere değerlendirme konularında en az üç yıllık tecrübeye sahip ya da değerlendirme konusunda yurt içinde veya yurt dışında yetkili kurumlar tarafından verilen mesleki yeterlilik sertifikalarına sahip olan kişileri ifade eder) Şirket bünyesinde yer alan ve Değerleme faaliyeti içerisinde aktif rol alan personelin yukarıda belirtilen şartlara sahip olduğu,
- Bankalardan gelen taleplerin değerlendirme çalışmasının gerekli düzeyde bilgi, mesleki yeterlilik ve beceriye sahip personel tarafından gerçekleştirildiği, Değerleme yapan Uzmanların, hizmetlerini yerine getirmek için gerekli bilgi birikimine, yeterliliğe ve deneyime sahip olduğu uzmanların yeterlilikleri konusunda yanıltıcı olmadığı ve ancak yeterliliğine uygun işleri kabul ettikleri.
- TUVEO Değerleme A.Ş nin, kalite güvence sisteminin işleyişinden sorumlu yönetim kurulu üyeleri ile değerlendirme faaliyeti ile iştigal eden personelinin bilgi ve yeteneklerinin yeterli olmadığı değerlendirme faaliyetlerini kabul etmediği. Değerleme faaliyetinin en iyi kalitede olabilmesi ve değerlendirme sonunda tam ve doğru bir görüş bildirilmesini sağlamak için, değerlendirme çalışmasının her aşamasında değerlendirmeyi yapan personelin takip edildiği, yönlendirildiği, gerekli görüldüğü hallerde ilave açıklamalar istendiği ve hazırlanan raporların Kontrol birimi tarafından kontrollerinin yapıldığı, Sorumlu Değerleme Uzmanı tarafından onaylandığı, raporların imzalı birer nüshalarının word ve pdf formatında elektronik ortamda arşivlendiği ve yedeklemelerinin yapıldığı, gelen taleplerin, talep anından raporlanması ve arşivlenmesine kadar izlenen tüm sürecin kayıt edildiği “Değerleme Süreç Takip Formu” düzenlendiği, raporlara ilişkin talep yazısı, tapu senedi, yapı ruhsatı ve vb. ekler ile saha çalışma formları gibi tüm belgelerin 10 yıl süre ile saklamak üzere banka, tarih ve rapor numarası takip edilerek tasnif edildiği ve elektronik ortamda arşivlendiği,
- Talepte bulunan Bankaya hazırlanacak olan Değerleme raporunun hazırlanmasında her aşamada ihtiyaç duyulması halinde konu ile ilgili Uzmanından görüş alındığı,
- Tam tarafsızlık ve bağımsızlık ilkelerine uygunluk içerisinde hizmet verildiği, hizmet verilen bankaların tam tarafsızlık ve bağımsızlık ilkelerine uygun şekilde davrandığı tarafsızlığı ve bağımsızlığı etkileyecek hiçbir olumsuz talebin olmadığı olumlu şartlarda tam tarafsızlık ve bağımsızlık ilkelerine uygunluk içerisinde hizmet verildiği, TUVEO DEĞERLEME olarak yukarıda belirtilen şartları yerine getirecek şekilde değerlendirme ile ilgili görevleri kabul edeceği ve Değerleme ilgili çalışmalarına aynı ilkelere bağlılıkla faaliyetine devam edeceği, Bu şartların yerine getirilebilmesi için tüm şartların uygun olduğu, bu hizmetlere ilişkin mesleki sorumluluk sigortasının düzenlendiği, gelen taleplerin karşılanabilmesi için uzman sayısının artırılması amacıyla nitelikli uzman personel temini çalışmalarının devam ettiği,
- Kalite Güvence Sisteminin Gözden Geçirilmesi için yapılan kontrol ve denetim sonucunda kalite Güvence Sistemine uygun olmayan şartlara rastlanmadığı, Tespit edilmiştir.



## 5.4 TUVEO KALİTE POLİTİKASI

TUVEO Kurumsal Gayrimenkul Değerleme ve Danışmanlık A.Ş. olarak dürüstlük, sorumluluk, bağımsızlık, tarafsızlık, liyakat, gizlilik, hızlılık ilkeleriyle Uluslararası Değerleme Standartlarında, yasalara, BDDK Yönetmeliklerine ve Sermaye Piyasası Kurulu tebliğlerine uygun hizmet vermek,

Kalite yönetim sistemini uygulayarak etkinliğini sürekli iyileştirmek, bununla beraber çalışanlarının mesleki ve kişisel gelişimine katkıda bulunarak müşteri memnuniyetini sürekli kılmak firmamızın kalite politikasıdır.

- **VİZYONUMUZ,**  
Uluslararası kalite ve standartlarda çalışan, gelişim ve başarıda sürekliliği yakalayan, İzmir başta olmak üzere Türkiye’den Dünya’ya açılan bilgi, donanım ve marka değeri olan değerlendirme şirketi olmak.
- **MİSYONUMUZ,**  
Kurumsal yaklaşım anlayışı altında, dürüst, ilkeli, disiplinli, özverili çalışma ortamı içinde, bağımsız – tarafsız, güvenilir ve elit değerlendirme hizmetini vermek, verimli ve karlı çalışmak.  
Toplam kalite yönetim sistemi anlayışı içinde yeni bilgi ve güncel teknolojileri kullanarak, çalışanların eğitimine ve kişisel gelişimine sürekli katkıda bulunarak, hizmet kalitesini, çalışan ve müşteri memnuniyetini arttırmaktır.

## 6. KALİTE GÜVENCE SİSTEMİNE EK OLARAK GELİŞTİRİLEN BİLGİ GÜVENLİĞİ POLİTİKASI

TUVEO Kurumsal Gayrimenkul Değerleme ve Danışmanlık A.Ş. olarak görevimiz ve konumuz gereği, bankalara ve kurumlara vermiş olduğumuz hizmetlerin gizliliği sebebiyle kasıtlı ve ya kasıtsız oluşabilecek güvenlik açıklarını engellemek amacı ile “Bilgi Güvenliği Politikası” oluşturularak tüm personele tebliğ edilmiştir.

### 6.1 BİLGİ GÜVENLİĞİ HAKKINDA 2012/3 NOLU TEBLİĞ İÇERİĞİ VE MADDELERİ

## TUVEO

### BİRİNCİ BÖLÜM Genel Hükümler

#### Amaç

**Madde 1-** Bu yönergenin amacı; TUVEO A.Ş.’nin görevi ve konumu nedeniyle bilgi çağı gereklerine paralel olarak bilgi paylaşımı ve güvenliği konularında tedbir almak, bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek, içeriden ve/veya dışarıdan gelebilecek kasıtlı veya kazayla oluşabilecek tüm tehditlerden korunmasını sağlamak ve yürütülen faaliyetleri etkin, doğru, hızlı ve güvenli olarak gerçekleştirmektedir.

#### Kapsam

**Madde2-** Bu yönerge, TUVEO A.Ş.’ye bağlı kadrolu ve çözüm ortağı tüm personelin, bilgi sistemleri kullanımına yönelik kurumsal ve kişisel bilgi güvenliği ilke kurallarını kapsamaktadır.

## İKİNCİ BÖLÜM BİLGİ GÜVENLİĞİ POLİTİKALARI

#### E-Posta Politikası

##### Madde 3-

(1)E-Posta ile ilgili yasaklanmış kullanım kuralları aşağıda belirtilmiştir.

a) Kullanıcı hesaplarına ait parolalar ikinci bir şahsa verilmemelidir.

- b) Şirket ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir.
- c) Kullanıcı, Şirketin e-posta sistemini taciz, suiistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajları göndermemelidir. Bu tür özelliklere sahip bir mesaj alındığında ilgili birime derhal haber verilmelidir.
- d) Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır. Diğer kullanıcılara bu amaçlar ile e-posta gönderilmemelidir.
- e) Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postal alındığında başkalarına ileilmeyip, ilgili birime haber verilmelidir.
- f) Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır. Kullanıcı, e-posta ile uygun olmayan içerikler (siyasi propaganda, ırkçılık, pomografi, fikri mülkiyet içeren malzeme, vb.) göndermemelidir.
- g) Kullanıcı, e-posta kullanımı sırasında dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip; suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.

(2)E-Posta ile ilgili kişisel kullanım kuralları aşağıda belirtilmiştir.

- a) E-posta kişisel amaçlar için kullanılmamalıdır.
- b) Kullanıcı, mesajlarının yetkisiz kişiler tarafından okunmasını engellemelidir. Bu yüzden parola kullanılmalı ve kullanılan parola en geç 45 günde bir değiştirilmelidir. E-posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunmalıdır.
- c) Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın ilgili birime haber vermelidir.
- d) Kullanıcı, kurumsal mesajlarını, kurum iş akışının aksamaması için cevaplandırmalıdır.
- e) Kullanıcı, kurumsal e-postalarının, kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesini ve okunmasını engellemelidir.
- f) Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar ilgili birime haber verilmelidir.
- g) 6 ay süreyle kullanılmamış e-posta adresleri kullanıcıya haber vermeden sunucu güvenliği ve veri depolama alanının boşaltılması için kapatılmalıdır.
- h) Kullanıcı parolaları, en az 8 karakterden oluşmalı ve parolalarının içinde; en az 1 tane harf, en az 2 tane rakam ve en az 1 tane özel karakter (@,^,+,\$,#,&,/,,{,\*,-,} ,=-.f,-.-) içermelidir.
- i) Kullanıcı, kendilerine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolalarının kırıldığını fark ettiği andan itibaren ilgili birime haber vermelidir.

(3)Kurumsal e-postalar yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.

(4)Kullanıcı, e-postalarına erişirken, POP3, SMTP, HTTP vb kullanıcı adı ve parolasını açık metin olarak (okunabilir halde) taşıyan protokolleri kullanmamalıdır.

(5)Kurum, e-postaların kurum bünyesinde güvenli ve başarılı bir şekilde iletilmesi için gerekli yönetim ve alt yapıyı sağlamakla sorumludur.

(6)Virüs, solucan, truva atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslere bulaşmış e-postalar antivirüs yazılımları tarafından analiz edilip, içeriği korunarak virüslerden temizlenmelidir. Ağa dâhil edilmiş bilgisayarlarda ve sunucularda ağ güvenlik yöneticileri bu yazılımdan sorumludur

## Parola Politikası

### Madde 4-

(1)Parola Politikası ile ilgili genel kurallar aşağıda belirtilmiştir.

- Sistem hesaplarına ait parolalar (bankaların rapor takip sistemleri, şirket içi rapor takip sistemi) en geç 6 ayda değiştirilmelidir.
- Kullanıcı hesaplarına ait parolalar (örnek, e-posta, web, masaüstü bilgisayar vs.) en geç 45 günde bir değiştirilmelidir.
- Sistem yöneticisi sistem ve kullanıcı hesapları için farklı parolalar kullanmalıdır.
- Parolalar e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- Kullanıcı, parolasını başkası ile paylaşmaması, kâğıtlara ya da elektronik ortamlara yazmaması konusunda bilgilendirilmeli ve eğitilmelidir.
- Kurum çalışanı olmayan kişiler için açılan kullanıcı hesapları da kolayca kırılmayacak güçlü bir parolaya sahip olmalıdır.
- Bir kullanıcı adı ve parolası, aynı anda birden çok bilgisayarda kullanılmamalıdır.

(2)Kullanıcı güçlü bir parola oluşturmak için aşağıdaki parola özelliklerini uygulamalıdır.

- En az 8 haneli olmalıdır.
- İçerisinde en az 1 tane harf bulunmalıdır. (a, b, C...)
- İçerisinde en az 2 tane rakam bulunmalıdır. (1, 2, 3...)
- ç) İçerisinde en az 1 tane özel karakter bulunmalıdır. (@, !,?,^,+,\$,#,&,İ,{,\*,-,=,....)
- Aynı karakterler peş peşe kullanılmamalıdır. (aaa, ll 1, XXX, ababab...)
- Sıralı karakterler kullanılmamalıdır. (abcd, qwert, asdf,l234,zxcvb...)
- İ) Kullanıcıya ait anlam ifade eden kelimeler içermemelidir. (Aileden birisinin, arkadaşının, bir sanatçının, sahip olduğu bir hayvanın ismi, arabanın modeli vb.)

(3)Şifre koruma standartları ile ilgili kurallar aşağıda belirtilmiştir.

- Bütün parolalar şirkete ve bağlı olduğu bankalara/kurumlara ait gizli bilgiler olarak düşünülmesi ve kullanıcı, parolalarını hiç kimseyle paylaşmamalıdır.
- Web tarayıcısı ve diğer parola hatırlatma özelliği olan uygulamalardaki "parola hatırlama" seçeneği kullanılmamalıdır.
- Parola kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir.
- Güvenlik taraması sonucunda parolalar tahmin edilirse veya kırılırsa kullanıcıdan parolasını değiştirmesi talep edilebilir.

(4)Uygulama Geliştirme Standartları

- Bireylerin ve grupların kimlik doğrulaması işlemini desteklemelidir.
- Parolalar metin olarak veya kolay anlaşılabilir formda saklanmamalıdır.
- Parolalar, şifrelenmiş olarak saklanmalıdır.

## Antivirüs Politikası

### Madde 5-

(1) Antivirüs Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a) Şirketin tüm istemcileri ve sunucuları antivirüs yazılımına sahip olmalıdır. Ancak sistem yöneticilerinin gerekli gördüğü sunucular üzerine istisna olarak antivirüs yazılımı yüklenmeyebilir.
- b) İstemcilere ve sunuculara virüs bulaştığı fark edildiğinde etki alanından çıkartılmalıdır.
- c) Sistem yöneticileri, antivirüs yazılımının sürekli ve düzenli çalışmasından ve istemcilerin ve sunucuların virüsten arındırılması için gerekli prosedürlerin oluşturulmasından sorumludur.
- d) Kullanıcı hiç bir sebepten dolayı antivirüs yazılımını bilgisayarından kaldırmamalıdır.
- e) Antivirüs güncellemeleri antivirüs sunucusu ile yapılmalıdır. Sunucular internete sürekli bağlı olup, sunucuların veri tabanları otomatik olarak güncellenmelidir. Etki alanına bağlı istemcilerin, otomatik olarak antivirüs sunucusu tarafından antivirüs güncellemeleri yapılmalıdır.
- f) Etki alanına dâhil olmayan kullanıcıların güncelleme sorumluluğu kendilerine ait olup, herhangi bir sakınca tespit edilmesi durumunda, sistem yöneticileri bu bilgisayarları ağdan çıkartabilmelidir.
- g) Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
- h) Optik Media ve harici veri depolama cihazları antivirüs kontrolünden geçirilmelidir.
- i) Kritik veriler ve sistem yapılandırmaları düzenli aralıklar ile yedeklenmeli ve bu yedekler farklı bir elektronik ortamda güvenli bir şekilde saklanmalıdır. Yedeklenen verinin kritik bilgiler içermesi durumunda, alınan yedekler şifre korumalı olmalıdır.

## İnternet Erişim ve Kullanım Politikası

### Madde 6-

(1) İnternet Erişim ve Kullanım Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a) Şirketin bilgisayar ağı, erişim ve içerik denetimi yapan ağ güvenlik duvar(lar)ı üzerinden internete çıkmalıdır. Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları önlemek üzere tasarlanan cihazlardır.
- b) Şirketin politikaları doğrultusunda içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler yasaklanmalıdır.
- c) Şirketin ihtiyacı doğrultusunda Saldırı Tespit ve Önleme Sistemleri kullanılmalıdır.
- ç) Şirketin ihtiyacı ve olanakları doğrultusunda antivirüs sunucuları kullanılmalıdır. İnternete giden ve gelen bütün trafik virüslere karşı taranmalıdır.
- d) Kullanıcıların internet erişimlerinde firewall, antivirüs, içerik kontrol vs. güvenlik kriterleri hayata geçirilmelidir.
- e) Çalışma saatleri içerisinde iş ile ilgili olmayan sitelerde gezinilmemelidir.
- f) İş ile ilgili olmayan (müzik, video dosyaları) dosyalar gönderilmemeli ve indirilmemelidir. Bu konuda gerekli önlemler alınmalıdır.
- g) Üçüncü şahısların internet erişimleri için misafir ağı erişimi verilmelidir.

## Sunucu Güvenlik Politikaları

### Madde 7-

(1) Sahip olma ve sorumluluklar ile ilgili kurallar aşağıda belirtilmiştir.

- a) Şirkette bulunan sunucuların yönetiminden, ilgili sunucuyla yetkilendirilmiş personel(ler) sorumludur.
- b) Sunucu kurulumları, konfigürasyonları, yedeklemeleri, yamaları, güncellemeleri sadece sorumlu personel(ler) tarafından yapılmalıdır.
- c) Tüm bilgiler, sistem yöneticisinin belirlediği kişi(ler) tarafından güncel tutulmalıdır.

(2) Genel yapılandırma kuralları aşağıda belirtilmiştir.

- a) Sunucu kurulumları, yapılandırmaları, yedeklemeleri, yamaları, güncellemeleri sistem yöneticisinin belirlediği kişi(ler) tarafından yapılmalıdır.
- b) Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- c) Servislere erişimler, kaydedilerek ve erişim kontrol yöntemleri ile koruma sağlanmalıdır.

ç) Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve antivirüs vb. koruma amaçlı otomatik olarak yazılımlar tarafından yapılmalıdır. Güncellemelerde değişiklik yapılacak ise bu değişiklikler, önce değişiklik yönetimi kuralları çerçevesinde, bir onay ve test mekanizmasından geçirilmeli, sonra uygulanmalıdır. Bu çalışmalar için yetkilendirilmiş bir personel olmalıdır.

d) Sunucular üzerinde lisanslı yazılımlar kurulmalıdır.

e) Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.

### Uzaktan Erişim Politikası

#### Madde 8-

(1) Uzaktan erişim politikası ile ilgili kurallar aşağıda belirtilmiştir.

a) Uzaktan erişim güvenliği denetlenmelidir.

b) Şirket çalışanları bağlantı bilgilerini hiç kimse ile paylaşmamalıdır.

c) Şirketin ağına uzaktan bağlantı yetkisi verilen çalışanlar veya sözleşme sahipleri bağlantı esnasında aynı anda başka bir ağa bağlı olmamalıdır.

d) Telefon hatları üzerinden uzaktan erişim, mümkün olan en üst düzeyde güvenlik yapılandırması ile kullanılmalıdır.

e) Kurum ağına uzaktan erişecek bilgisayarların işletim sistemi ve antivirüs yazılımı güncellemeler yapılmış olmalıdır.

f) Kurumdan ilişigi kesilmiş veya görevi değişmiş kullanıcıların gerekli bilgileri yürütülen projeler üzerinden otomatik olarak alınmalı, yetkiler ve hesap özellikleri buna göre güncellenmelidir.

### Bilgi Sistemleri Genel Kullanım Politikası

#### Madde 9-

(1) Bilgi sistemlerine sahip olma ve bu sistemleri genel kullanım kuralları aşağıda belirtilmiştir.

a) Şirketin güvenlik sistemleri kişilere makul seviyede mahremiyet sağlasa da, Şirketin bünyesinde oluşturulan tüm veriler Şirketin mülkiyetindedir.

b) Kullanıcılar bilgi sistemlerini kişisel amaçlarla kullanmamalıdır. Bu konuda ilgili politikalar dikkate alınmalıdır.

c) Şirket, bu politika çerçevesinde ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

d) Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı ve kopyalanmamalıdır.

e) Sorumlu bilgi işlem personeli ve ilgili teknik personel haricindeki kullanıcılar tarafından ağa bağlı cihazlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri gibi ayarlar değiştirilememelidir.

f) Bilgisayarlara lisanssız program yüklenmemelidir.

g) Gereksizlikçe bilgisayar kaynakları paylaşımına açılmamalıdır. Kaynakların paylaşımına açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

(2) Bilgi sistemleri genel yapılandırması ile ilgili kurallar aşağıda belirtilmiştir

a) Dizüstü bilgisayarın çalınması/kaybolması durumunda, durum fark edildiğinde en kısa zamanda ilgili birime haber verilmelidir.

b) Kullanıcılar tarafından gönderilen e-postalarda gereğine göre aşağıdaki şekilde bir açıklama yer almalıdır.

**“Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşırsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminden siliniz. TUVEO A.Ş. bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmemektedir.”**

c) Kullanıcılar ağ kaynaklarının verimli kullanımı konusunda dikkatli olmalıdır. E-posta ile gönderilen büyük dosyaların sadece ilgili kullanıcılara gönderildiğinden emin olunmalı ve mümkünse dosyalar sıkıştırılmalıdır.

## Donanım ve Yazılım Envanteri Oluşturma Politikası

### Madde 10-

(1) Donanım ve yazılım envanteri oluşturma ile ilgili kurallar aşağıda belirtilmiştir.

- Oluşturulan envanter tablosunda şu bilgiler olmalıdır; sıra no, bilgisayar adı, bölüm, marka, model, seri no, özellikler, ek aksesuarlar, işletim sistemi, garanti süresi vs.
- Bu tablolar merkezi bir web sunucuda tutulmalı ve belirli aralıklarla güncellenmelidir. İlgili siteye girişler güvenlik politikaları çerçevesinde yapılmalıdır.
- Envanter bilgileri sık sık kontrol edilmelidir. Bu şekilde bilgi eksikliğinin yol açacağı kayıp ve maliyetlere engel olunmalıdır.

## Kriz-Acil Durum Politikası

### Madde 11-

(1) Acil Durum politikası ile ilgili kurallar aşağıda belirtilmiştir.

- Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümanite edilmelidir.
- Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Problem durumlarında sistem kesintisiz veya makul kesinti süresi içerisinde felaket ve/veya iş sürekliliği merkezi üzerinden çalıştırılabilir.
- Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
- Acil durumlarda sistem kayıtları incelenmek üzere saklanmalıdır.
- Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
- Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
- Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
- Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili birimlere iletilmelidir.

## Fiziksel Güvenlik Politikası

### Madde 12-

(1) Fiziksel Güvenlik ile ilgili kurallar aşağıda belirtilmiştir.

- Şirket alarm sistemi ile koruma altında tutulmalı, şirkete giriş çıkışlar personele özel şifreler ile takip edilmelidir.
- Şirketin bilgi varlıklarının depolandığı arşiv odası kilit altında tutulmalı ve oda içinde kilitli çelik dolap içinde muhafaza edilmelidir. Yetkili personel dışında arşive erişim olmamalıdır.
- Fotokopi, yazıcı vs. türü cihazlar mesai saatleri dışında kullanıma kapatılmalı, mesai saatleri içerisinde yetkisiz kullanıma karşı koruma altına alınmalıdır.
- Çalışma alanlarının kullanılmadıkları zamanlarda kilitli ve kontrol altında tutulması temin edilmelidir.

## Kimlik Doğrulama ve Yetkilendirme Politikası

### Madde 13-

(1) Kimlik Doğrulama ve Yetkilendirme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- Şirket ve bağlı olduğu banka sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümanite edilecektir.
- Şirket ve bağlı olduğu banka sistemlerine erişmesi gereken firma kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümanite edilecektir.
- Şirket bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümanite edilmeli ve denetim altında tutulmalıdır.

- d) Tüm kurumsal sistemler üzerindeki kullanım hakları periyodik olarak gözden geçirilmeli ve bu gereksinimler gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
- e) Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.

### Bilgi Sistemleri Yedekleme Politikası

#### Madde 14 –

(1) Bilgi Sistemleri Yedekleme Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a) Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli olarak alınması kontrol altında tutulmalıdır.
- b) Dijital ve basılı olarak yedeklenen veriler en az 10 yıl arşivlenerek fiziksel güvenliği sağlanmış çelik dolaplarda, kilit altında tutulmalıdır.
- c) Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
- d) Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
- e) Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
- f) Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dâhilinde tamamlanması gerekmektedir.

### Personel Güvenliği Politikası

#### Madde 15-

(1) Personel Güvenliği Politikası ile ilgili kurallar aşağıda belirtilmiştir.

- a) Çeşitli seviyelerdeki bilgiye erişim hakkının verilmesi için personel yetkinliği ve rolleri kararlaştırılmalıdır.
- b) 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.
- c) İş tanımı değişen veya Kurumdan ayrılan kullanıcıların erişim hakları kaldırılmalıdır.

## ÜÇÜNCÜ BÖLÜM POLİTİKANIN İHLALİ VE YAPTIRIMLAR

### İhlal ve Yaptırımlar

#### Madde 16-

(1) Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince sırası ile uygulanacak yaptırımlar aşağıda belirtilmiştir.

- a) Uyarma
- b) Kınama
- c) Sözleşme feshi

Tebliğ Eden;

TUVEO Kurumsal Gayrimenkul  
Değerleme ve Danışmanlık A.Ş.

Tebellüğ Eden;

TUVEO Kurumsal Gayrimenkul  
Değerleme ve Danışmanlık A.Ş.

**Tablo (Ek-1)**  
**Kısaltmalar Tablosu**

Kısaltma	Tanım
Zincir e-posta	Bir kullanıcıya gelen şans ve para kazanma yöntemleri gibi bir içeriğe sahip e-postanın art arda diğer kullanıcılara gönderilmesi
Spam	Yetkisiz ve/veya istenmeyen reklam içerikli e-postalar
Sahte e-posta	Başka bir kişi gibi davranarak ve gerçek göndereni maskeleyerek kişinin güvenini kazanmak ve kişisel bilgilerine (tamamen yasadışı yoldan) erişmek
Risk	Kurumun bilgi sistemlerinin gizliliğini, mevcudiyetini ve bütünlüğünü etkileyen faktörler
Yedekleme	Ekipmanın bozulması durumu düşünülerek dosyaların ve/veya veritabanının başka bir yere kopyalanması işlemi
Veritabanı	Kolayca erişilebilecek, yönetilebilecek ve güncellenebilecek şekilde düzenlenmiş olan bir veri topluluğu
Şifreleme	Veriyi, istenmeyen kişilerin anlayamayacakları bir biçime sokan Özel bir algoritma

## 7. KALİTE GÜVENCE SİSTEMİNİN İŞLEYİŞİNDEN SORUMLU YÖNETİM KURULU ÜYESİNE İLİŞKİN BİLGİLER;

### Eğitim;

- EGE ÜNİVERSİTESİ ZİRAAT FAKÜLTESİ
- PE BATALAS LEAD ACCESSOR SERTİFİKASI
- TS EN ISO 9001 TEMEL EĞİTİMİ
- TS EN ISO 9001 DÖKÜMANTASYON EĞİTİMİ
- TS EN ISO 9001 İÇ TETKİKİÇİ EĞİTİMİ
- TS EN ISO 22000 GIDA GÜVENLİĞİ YÖNETİMİ SİST. EĞİTİMİ
- TS EN ISO 14001 GIDA ÇEVRE YÖNETİMİ SİST. EĞİTİMİ
- TS ISO 18001 İŞ SAĞLIĞI VE GÜVENLİĞİ YÖNETİMİ SİST. EĞİTİMİ

### Tecrübesi;

- 1992-2007 Türk Standartları Enstitüsü Ürün Belgelendirme Uzmanı, ISO 9000 ve ISO 22000 Denetimcisi
- 2007-Halen TUVEO A.Ş. Yönetim Kurulu Üyesi – Kalite Güvence Sistemi Sorumlusu

Saygılarımla,

Zuhal ÇERÇİ  
Yönetim Kurulu Üyesi  
Kalite Güvence Sorumlusu