BİLGİ GÜVENLİĞİ POLİTİKAMIZ

- ✓ Bilgi Güvenliği Yönetim Sistemimiz ile tüm faaliyetlerimizin ISO 27001:2013 standardına uygun yürütülmesini garanti altına almak,
- ✓ İlgili tarafların bilgi varlıklarına güvenli bir şekilde erişimini sağlamak,
- ✓ İçeriden veya dışarıdan, bilerek ya da bilmeyerek meydana gelebilecek her türlü tehdide karşı Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş.'nin ve müşterilerinin bilgi varlıklarını korumak, bilginin kullanılabilirliğini, gizliliğini, bütünlüğünü bozmaya çalışacak yetkisiz kişilerin erişimine karşı korumak, bilgiye erişebilirliği iş prosesleriyle gerektiği şekilde sağlamak,
- ✓ Bilgi Güvenliği konusunda personele bilgi vererek bilinçlendirmeyi sağlamak,
- ✓ Bilgi Güvenliğindeki gerçekte var olan veya şüphe uyandıran tüm açıkların, şirket yöneticilerine bildirilmesi ve gerekli tedbirlerin alınmasını sağlamak,
- ✓ Bilgiye erişebilirlik ve bilgi sistemleri için iş gereksinimlerini karşılamak,
- ✓ İlgili tarafların bilgi varlıkları üzerinde oluşabilecek risklerini değerlendirmek ve yönetmek,
- ✓ Kurumun güvenilirliğini ve marka imajını korumak,
- ✓ Bilgi güvenliğinin ihlali durumunda gerekli görülen yaptırımları uygulamak,
- ✓ Tabi olduğu ulusal, uluslararası veya sektörel düzenlemeleri, yasal ve ilgili mevzuat gereklerini yerine getirmek, anlaşmalardan doğan yükümlülükleri karşılamak, ilgili taraflara yönelik kurumsal sorumluluklarından kaynaklanan bilgi güvenliği gereksinimlerini sağlamak,
- ✓ İş / Hizmet sürekliliğine bilgi güvenliği tehditlerinin etkisini azaltmak ve işin sürekliliğini ve sürdürülebilirliğini sağlamak,
- ✓ Kurulan kontrol altyapısı ile bilgi güvenliği seviyesini korumak ve iyileştirmek,
- ✓ Çalışanların, tedarikçilerin ve iş ortaklarının bilgi güvenliği bilincini geliştirmek.

Yürütme Kurulu Üyesi

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ

AMAÇ:
Bu politika; yetkili kullanıcı erişimini sağlamak ve yetkisiz erişimi önlemek amacıyla oluşturulmuştur.

KAPSAM:
AVRUPA sisteminde, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan basamaklardır.

UYGULAMA:
1. Personel kendilerine tahsis edilen cihazlar ile kullanıcı denetimi ve izni ile network'e giriş yapabilir. Müşterilerin sistemleri ve web tabanlı sistemlere ise network'e giriş yapma ihtiyacı duymadan kendileri için belirlenmiş kullanıcı adı ve şifreler ile giriş yapabilmektedirler.

2. Firma içerisinde kullanılan ana makinadaki İşletim Sisteminde tüm bilgisayarların kullanıcı tanımlarının ve erişim yetkileri aktif dizinde oluşturulmuştur.

3. Kullanıcı yetkilendirilmeleri kullanıcı bazında yapılmıştır.

4. Bölüm ihtiyaçları göz önünde bulundurularak oluşturulan bazı yetkililer hariç olmak üzere tanımlanan kullanıcıların donanım ihtiyaçları (floppy, usb, cd-writer, cd-rom vb.) yasaklanmıştır.

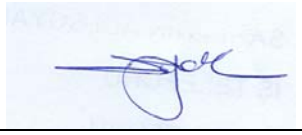
5. Aktif dizine bağlanan kullanıcı parolaları bilgi işlem tarafından 128 bit olarak verilmektedir.

6. Firma içerisinde kullanılan ETA, İNVEKS ve Intranet(KUBA) programları için de benzer yetkilendirme kendi içerisinde yapılmıştır. Her çalışan kendi kullanıcı adı ve şifresi ile sisteme girebilmektedir. Yetkilendirme sadece Bilgi İşlem Yetkilileri tarafından yapılmaktadır.

7. Yetkiler, ilgili birim için "Muhasebe", "Yönetim" ve "Çalışan" olarak belirlenmiş ve yetkilendirme yapılmıştır.

8. Erişim gereksinimi artık kalmamış kullanıcılar için bu personelin kullanıcı adı ve erişim şifresi silinir.

9. Ağ Erişim Denetimi
9.1. Ağ üzerinde aktif dizin kullanıcıları için "data", "yönetim", "muhasebe" sürücüleri oluşturulmuştur.
9.2. her sürücü yetki grupları ve kullanıcılara göre yetkilendirilmiştir.
9.3. Kullanıcılara göre dosya erişimi, silme-ekleme yetkisi tanımlanmıştır.
9.4. "data" sürücüsü üzerinde ortak kullanıma açık dizinler oluşturulmuştur. Bu dizinlere erişim açıktır.
9.5. Paylaşımlar Sistem Yöneticisi tarafından belirlenmektedir.
9.6. "data" dizinine tüm kullanıcıların dosya oluşturma, ekleme, değiştirme yetkisi bulunmaktadır.
9.7. İSO formları "data" dizini altında oluşturulan "kalite" dizininde ve intranet sisteminde tutulmaktadır. Bu dizinine ve intranet sisteme tüm kullanıcılar erişebilmekte ancak sadece okuma yetkisine sahiptirler. Kalite Birimi dışında kullanıcıların dosya ve/veya form oluşturma, ekleme, değiştirme yetkisi bulunmamaktadır. Bu şekildeki istekleri var ise kalite birimine haber verilir.

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ
	

9.8. “kalite” dizinine sadece Kalite Birimine ait üye kullanıcılarının dosya oluşturma, ekleme, değiştirme yetkisi bulunmaktadır. Silme yetkileri yoktur.
9.9. Ağ bağlantıları için kullanıcı parolaları Bilgi İşlem tarafından verilmektedir.
10. ETA Muhasebe sistemi
10.1. ETA Muhasebe sistemi ayrı bir sunucu üzerinde tutulmaktadır.
10.2. Program kullanıcıları kendileri için program içinde özel olarak oluşturulmuş kullanıcı adı ve şifresiyle giriş yapmaktadır.
10.3. Tüm kullanıcılar kendi kişisel kullanımları için benzersiz bir kimliğe sahiptirler.
10.4. Muhasebe departmanı için “muhasebe” dizini ve muhasebe ağı oluşturulmuştur. Bu ağ dışındakiler hem bu programa hem de “muhasebe” dizinine ulaşma yetkileri yoktur.
10.5. Kullanıcıların bağlantı süresinde bir kısıtlama yapılmamıştır.

11. INVEX ve Intranet(KUBA) programları
11.1. Her iki program da web tabanlı olup bu programlar için dışarıdan hizmet alınmaktadır.
11.2. Programlara ulaşım için kullanıcıların Avrupa Aktif Dizinine ve ağa bağlanmaları şart değildir.
11.3. Her iki program için tüm kullanıcılar farklı kullanıcı adı ve şifresiyle giriş yapabilmektedirler.
11.4. her iki program için kullanıcı oluşturma, değiştirme ve silme yetkisi Bilgi İşlem bölümündedir.
11.5. her iki program için kullanıcılar kullanıcı bazında yetkilendirme yapılmaktadır. Kullanıcılar yetkileri doğrultusunda veri görebilir, değiştirebilir ve silebilirler.

12. İnternet Erişimi
12.1. İnternet erişimi Firewall üzerinde Yönetim tarafından belirli politikalara bağlanmıştır.
12.2. Avrupa network içindeki veri alışveriş hızını düşürmemek ve boyutunu artırmamak amacıyla sosyal medya, kişisel mail ve video paylaşım sitelerine erişimleri kısıtlanmıştır.
12.3. Şirket bünyesi dışında olan kişiler şirkete geldiklerinde sadece “Avrupa misafir” kablosuz ağından internete ulaşabilmektedirler. “Avrupa misafir” ağı tüm ağlardan ayrı olarak planlanmış bir ağdır.

	TEMİZ EKRAN VE TEMİZ MASA POLİTİKASI	Doküman No : BGP/03 İlk Yayın Tarihi : 30.03.2019 Rev. No : 00 Rev. Tarihi : Sayfa No : 1 / 1

AMAÇ

Normal çalışma süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kâğıtlar ve depolama ortamları ve kişisel bilgisayarlar için gerekli şartları tanımlamak.

UYGULAMA

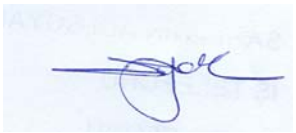
1. Ulaşılması istenmeyen bilgi ya da belgeler uygun olan yerlerde, kağıt ve bilgisayar ortamı, kullanılmadığında uygun kilitli dolaplarda muhafaza edilir.

2. Ağa bağlı bilgisayarlar başıboş olduklarında oturum açık olarak bırakılmazlar. Masasından ayrılan personel “Windows+ L” tuşlarına basarak ağ oturumunu otomatik olarak kilitlerler.

3. Hassas ve önemli iş bilgileri ya da belgeleri, gerekmedikleri zamanda özellikle de büro boş olduğunda, kilitlenir.

4. Gelen ve giden faks mesajları faks makinelerinde başıboş bırakılmaz. Elektronik olarak kaydedilen faks mesajlarına sadece yetkili kişiler ulaşabilmektedir.

5. Yazıcılar ve fotokopi makineleri belirli kullanıcılara ve farklı ağlara göre erişim yetkileri verilmiştir.

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ
	

	E-MAIL POLİTİKASI	Doküman No : BGP/04 İlk Yayın Tarihi : 30.03.2019 Rev. No : 00 Rev. Tarihi : Sayfa No : 1 / 1

AMAÇ

Bu politikanın amacı; AVRUPA ya gelen, giden e-postaların (e-mail) güvenliğini kontrol altına alarak güvenli olmayan ya da uygunsuz mesaj gönderimini ya da gelmesini engellemektir.

UYGULAMA

1. Firma içerisinde kişiler birbirlerine çok yakın otursalar dahi karşılıklı konuşmak yerine e-mail yazmayı tercih etmelidirler.

2. Gönderilecek e-mailler kısa, açık ve anlaşılır olmalıdır. Mesaj, birden fazla kişiye gidecek ise konunun gerçekten mesaj gidecek kişileri ilgilendirip ilgilendirmediğine dikkat edilir. Konu ile sadece haberdar olması gerekli kişiler “cc” bölümüne yazılır.

3. Mesajın gönderildiği kişiler mümkün olduğu kadar kısıtlı tutulur. “cc” kısmına gerçekten gerekli olmayan kişiler eklenmez.

4. Mesaj birden fazla kişiye gönderiliyor ve bu farklı kişilerin birbirinden haberdar olması gerekmiyor ise “To” kısmı yerine “Bcc” kısmı kullanılır.

5. Mesaj karşılığı verilmek istendiğinde gereksiz adresler ve gerekmiyor ise orijinal mesaj silinir.

6. Herhangi bir dağıtım listesinden (birçok kişiye gönderilen toplu mail adresleri) gelen bir ilan ya da bildiriye cevap (reply) vermek istendiğinde mesajın gerekmiyor ise tüm liste abonelerine değil de sadece bildiri sahibine gittiğinden emin olunur.

7. Boyutu büyük gönderimler için dosya sıkıştırıcı programlar kullanılır.

8. “Urgent” (acil) ibaresi gerekmedikçe kullanılmaz.

9. Kişileri kışkırtıcı, onur kırıcı, kutsal inançlara saldıran, ırkçı, karalayıcı, müstehcen ya da benzeri mesajlar gönderilmez.

10. Mesajın ulaştığından emin olunmak isteniyorsa teyit ettirilir.

11. Zincir mesajlar kesinlikle gönderilmez. (örn: “ Bu mesajı x kadar kişiye gönderirseniz y gün sonra bir dileğiniz gerçekleşecek” türünde yazılar içeren mesajlar)

12. Çok gizli bilgi içeren mesajlar gönderilemez.

13. Firmanız dışına göndereceğiniz toplu mesajlara fazlası ile dikkat edilir.

14. Alınan e- maillerin göndericisine dikkat edilir. Gönderenin kim olduğu bilinmeyeni alışık olunmayan, beklenmeyen mesajlara şüphe ile yaklaşılır. Bu tarz mesajlar virüs taramasından geçirildikten sonra açılır.

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ

	TAŞINABİLİR CİHAZLARIN KULLANIM POLİTİKASI	Doküman No : BGP/05 İlk Yayın Tarihi : 30.03.2019 Rev. No : 00 Rev. Tarihi : Sayfa No : 1 / 1

AMAÇ
Kurum içerisindeki taşınabilir bilgi işlem cihazlarının kullanım şartlarını belirlemek.

KAPSAM
Kurum içerisinde kullanılan tüm taşınabilir bilgi işlem cihazlarını kapsar.

UYGULAMA

Personel, bağlı olduğu birimin yöneticisi yazılı izin vermediği sürece hiçbir bilgi varlığını kurum dışına çıkaramaz.

Taşınabilir bilgi işlem araçlarının halka açık ve korumasız ortamlarda kullanılmasının gerektiği yerlerde, bilginin yetkisiz kişilerin eline geçmemesi için gerekli güvenlik önlemleri alınır.

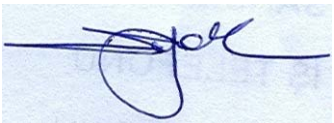
Taşınabilir bilgi işlem araçlarının üzerinde virüslere karşı koruyucu programlar güncel halde bulundurulur.

Taşınabilir bilgi işlem araçları sadece yetkilendirilmiş personel tarafından veriliş amaçlarında uygun şekilde kullanılır.
Uzaktan güvenli erişim için VPN sistemi kullanılır.

Taşınabilir cihazın kaybedilmesi ve/veya çaldırılması durumunda birim yöneticisi en kısa sürede haberdar edilir.

Genel Konular:
1. Dizüstü bilgisayar kullanıcıları hazırlanan taşınabilir cihazlar kullanım politikasını duyurularla bilgilendirilmiştir.
2. Dizüstü bilgisayarların kullanımı konusunda Bilgi İşlem bölümü tarafından tüm personele bildirim yapılacaktır.
3. Dizüstü bilgisayar kullanıcıları bilgisayarlarını Bilgi İşlem Bölümün' den zimmet belgesi imzalayarak almaktadır. Geri iade edilirken zimmet belgesinde belirtilen tüm aksesuarları ile birlikte teslim edecektir. (Çanta-Fare vs.)
4. Dizüstü Bilgisayar üzerlerine demirbaş numarası gösterir etiket basılacaktır.

Güvenlik Konuları;
1. Kurum bilgi işlem ağına sadece izin verilmiş dizüstü bilgisayarlar bağlanacak, şahsi bilgisayarlar kesinlikle bağlanmayacaktır.
2. Kuruma ait taşınabilir bilgisayarlarda sadece yapılan ise yönelik doküman/dosyalar islenebilecektir.
3. Taşınabilir bilgisayarlar gözetimsiz bırakıldıklarında fiziksel olarak emniyete alınacak, işletim sistemi erişimi kitlenecektir.
4. Ağa bağlı dizüstü bilgisayarlarda islenilen bilgi kendi harddisklerinde depolanmayacaktır. Üzerinde işlem yapılacak doküman merkezi dosya sunumcusundan bilgisayar harddiskine alınarak düzenlemeler yapıldıktan sonra tekrar sunumcuya kopyalanacaktır.Dizüstü bilgisayarların virüs programı ve işletim sistemleri güncellemelerinin yapılabilmesi için ağa bağlı olmasa dahi teknik hizmetlerden destek alınarak işlemlerin tamamlanması sağlanacaktır.

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ
	

	BİLGİ GÜVENLİĞİ İHLAL OLAYI POLİTİKASI	Doküman No : BGP/06 İlk Yayın Tarihi : 30.03.2019 Rev. No : 00 Rev. Tarihi : Sayfa No : 1 / 1

AMAÇ
Bilgi Güvenliği ihlal olayı vuku bulduğunda yapılacak tüm işlemleri belirlemektir.

KAPSAM
Bu olayın oluştuğu andan itibaren sistemi eski haline getirmekle görevli bilgi işlem merkezi ve diğer departman personelini kapsamaktadır.

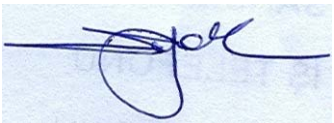
UYGULAMA

Bilgi Güvenliği Olayları ve Zayıflıklarının Rapor Edilmesi

1. Bilgi güvenliği olaylarının en hızlı biçimde rapor edilmesi için uygun hiyerarşik kanal mekanizmaları oluşturulacaktır. Her personele bu mekanizmalar bildirilerek karşılaşılan durumun ne şekilde rapor edileceği öğretilecektir.
2. Yapılacak sözleşmelerde tüm çalışanların, yüklenici ve üçüncü tarafların, sistem ve hizmetlerdeki gözledikleri veya şüphelendikleri herhangi bir güvenlik zayıflığına dikkat ederek rapor etmeleri istenecektir.

Bilgi Güvenliği İhlal Olayları ve İyileştirmelerinin Yönetilmesi

1. Bilgi güvenlik ihlal olayı oluşması durumunda ne şekilde işlem yapılacağı tüm senaryolar üzerinden geçilerek sorumlularla birlikte dokümante edilecektir.
2. Öncelikle planlı bir şekilde çalışma yapılabilmesi için ihlal olaylarının türleri, miktarları ve kuruma maliyetlerini ölçüp, izlemeye yarayan mekanizma kurulacaktır. Bunun için olay meydana geldiğinde hızlı bir şekilde BGYS ekibi toplanacaktır.
3. Sistemin zararlarının giderilip eski haline dönmesi konusunda yapılan plan ve ihtiyaçlar rapor halinde yönetim kuruluna sunulacaktır. Alınan karara binaen sorumluları ile birlikte kontroller uygulanacak, bu durumun tekrar yaşanmaması amacıyla gerekli iyileştirmeler yapılacaktır.
4. Bilgi güvenliği ihlal olaylarında mevcut izleme programları sayesinde alınacak kanıtlar toplanacak ve ilgili makama sunulacaktır. Bunun kanun karsısında kanıt olarak sunulabilmesi için gereksinimleri sağlayacak şekilde sistem kurulacaktır.

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ
	

1. Personel tarafından kurum dışına ticari herhangi bir bilgi, vb. çıkarılmayacak, çıkarılması gereken durumlarda ise sadece kurum donanımları ile taşıma sağlanacaktır.
2. Şahsi laptop, usb flashdisk vb. gibi taşınabilir ortamlar ile kurum dışında bilgi aktarımı gerçekleştirilmeyecektir.
3. Çıkarılması gerekli durumlarda aşağıdaki form doldurularak kurumun bilgisi ve onayı dahilinde kuruma ait taşınabilir ortamlar ile gerçekleştirilecektir.
4. Kurum dışında çalışma yapılacak hallerde, o lokasyonla kurum arasında VPN yapısı kurulacak ve taşınabilir bilgisayarlar bu VPN üzerinden sistemle iletişime geçecektir.
5. Bu politikanın sorumlusu BGYS Sorumlusudur.

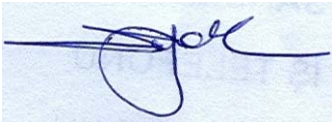
Kuruma Ait Taşınabilir Ortam: **Notebook ise kullanıcı adı ile**	*(dizüstü, flashdisk, cd,dvd vs.)*		
Ortam İçeriği:	*(…modülü güncelleme, kurulum kodu vs.)*		
Gideceği Kurum/Yer, Nedeni :			
Personel Adı Soyadı :			
Personel İmza:		**Tarih:**	
<u>Onaylayan</u> **Adı-Soyad:** **İmza:**			

	YÖNETİMİN BİLGİ GÜVENLİĞİ YÖNETİMİ SİSTEMİNE BAĞLILIK BEYANI	**BYN-01** **Yayın Tarihi: 30.03.2019** **Rev. Tarihi:** **Rev.No: 00**

AVRUPA Gayrimenkul Değerleme ve Danışmanlık A.Ş., Bilgi Güvenliği Yönetim Sistemi Politikası belgesinde ifadesini bulan çerçeve içinde Bilgi Güvenliği Yönetim Sisteminin (BGYS) kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, bakımına ve iyileştirilmesine olan bağlılığını aşağıdaki hususları gerçekleştirerek kanıtlayacağını beyan eder:

- BGYS amaçları ve planları kurulacaktır.
- Bilgi güvenliği için rolleri ve sorumlulukları kurulacak ve tanımlanacaktır.
- Risk analizlerini yapacak, analiz sonuçlarına bağlı olarak risk değerlendirmelerini ve risk ölçütlerini ortaya koyacak, bu çerçevede risk yönetimi sağlanacaktır.
- Bilgi güvenliği amaçlarını karşılamanın ve bilgi güvenliği politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi tanımlanacaktır.
- BGYS'yi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için yeterli kaynakları (finansal, insan kaynakları, ekipman, yazılım, danışmanlık, eğitim vs.) sağlanacaktır.
- Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirlemek üzere gerekli çalışmalar organize edilecek ve yönetilecektir.
- Sözleşme yapılan kurum / kuruluşlarda BGYS kapsam ve sınırları içinde kurum / kuruluş dâhilinde iç BGYS denetimleri gerçekleştirilecektir.
- Sözleşme yapılan kurum / kuruluşlarda BGYS kapsam ve sınırları içinde kurulan BGYS'nin denetimleri ve kontrolleri sonucu ortaya çıkan raporlarla, önleyici ve düzeltici faaliyetlerin raporları üst yönetim tarafından gözden geçirilecek, sürekli iyileştirme yaklaşımına dayalı olarak düzeltici ve önleyici faaliyetler gerçekleştirilecek, izlenecek, çözüm bekleyen sorunlar sonuçlandırılacaktır.

YÜRÜTME KURULU ÜYESİ

Hazırlayan **BGYS SORUMLUSU**	**Onaylayan** **YÜRÜTME KURULU ÜYESİ**	**ISO 27001** 1/1
		

1.Tanım

BGYS politikamızda Bilgi Güvenliği AVRUPA'nın bilgi varlıklarının aşağıdaki özelliklerinin korunması olarak tanımlanır:

Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması,
Bütünlük: Bilginin yetkisiz değiştirmelerden korunması ve değiştirildiğinde farkına varılması,
Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an kullanılabilir olması.

2.Kapsam

AVRUPA, Gayrimenkul Değerleme ve Kentsel Dönüşüm hizmetleri ofis alanlarının ilgili tüm unsurları ile ofis faaliyetlerinde kullanılan tüm donanım, yazılım ve personeli ile, AVRUPA Bilgi İşlem altyapısını kullanmakta olan tüm birimleri, üçüncü taraf olarak bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcılarını kapsamaktadır.

Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş. çalışanları değerleme hizmetinin değişik aşamaları sırasında hem hizmet vermekte olduğu müşterilerinin kendileri için hazırlanmış olan veri tabanlarına, hem de şirket içi veri tabanı programı ve bilgi saklama/yedekleme ortamlarına ulaşabilmektedirler. Avrupa A.Ş çalışanları, hizmet verilen kişi, kurum ve kuruluşların güvenini temin etmek ve verdiği hizmetler için kullandığı bilgi varlıklarını, gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamakla yükümlüdür.

3.Hedef

AVRUPA Yönetimi:
• Kurumun güvenilirliğini ve temsil ettiği makamın imajını korumak,
• Üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunluğu sağlamak,
• Kurumun temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak
Amacıyla kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler.

Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş. çatısı altında Bilgi Güvenliği politikasının hedefi; iş sürekliliğini sağlamak, bilgi güvenliği ile ilgili olarak meydana gelen güvenlik ihlallerinin etkilerinin önlenmesi veya en aza indirilmesiyle, konuyla ilgili olarak tüm çalışanların bilgi sahibi olması ve iş kayıplarını mümkün olan en düşük seviyeye çekmektir.

4.Çerçeve

AVRUPA risk yönetim çerçevesi, bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini, işlenmesini kapsar. Risk değerlendirmesi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Bu planın yönetiminden ve gerçekleştirilmesinden Bilgi Güvenliği Ekibi sorumludur.

5.İlkeler

Kurum bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes:
- ✓ Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı,
- ✓ Kritiklik düzeylerine göre işlediği bilgiyi yedeklemeli,

- ✓ Risk düzeylerine göre belirlenen güvenlik önlemlerini almalı,
- ✓ Bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi Güvenliği Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır.
- ✓ Kurum içi bilgi kaynakları (duyuru, doküman vb.) yetkisiz olarak 3.kişilere iletilemez.
- ✓ Kurum bilişim kaynakları, T.C. yasalarına ve bunlara bağlı yönetmeliklere aykırı faaliyetler amacıyla kullanılamaz.

6.Sorumluluklar

AVRUPA tüm çalışanları ve BGYS de tanımlanan dış taraflar, bu politikaya ve bu politikayı uygulayan BGYS politika, prosedür ve talimatlarına uymakla yükümlüdür. Birimlerin güvenlik sorumlularından oluşan Bilgi Güvenliği Ekibi, BGYS altyapısını desteklemek ve işleyişini devam ettirmekle sorumludur.

Şirket e posta sistemi, taciz, suiistimal veya herhangi bir şekilde şirket haklarına zarar vermeye yönelik öğeleri ve mesajları içeremez.

Zincir mesajlar veya mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında hemen silinir ve kesinlikle başkalarına iletilemez.

Kişisel kullanım için internetteki liste ve sitelere üye olunması durumunda kurum e-posta hesapları kullanılamaz.

Çalışanlar e-posta hesapları ile uygun olmayan içerikler (pornografi, ırkçılık, siyasi propaganda, fikri mülkiyet içeren malzeme vb) gönderemezler.

Çalışanlar, kendilerine gönderilen mesajların yetkisiz kişiler tarafından okunmasını, bu kişilerin mesaj içeriğiyle ilgili bilgi sahibi olmalarını engellemekle sorumludurlar.

Çalışanlar kendilerine özel hazırlanmış olan her türlü veritabanı kullanıcı adı ve şifrelerinin güvenliğini sağlamakla yükümlüdürler. Şifre ve kullanıcı adlarını unuttukları ya da kaybettiklerinde durumu acilen yetkililer bildirmekle yükümlüdürler.

Bütün bilgisayarlarda anti virüs programı kurulu olup, hiçbir kullanıcı programı etkisiz hale getiremez veya kaldırmazlar.

İşle ilgili olmayan (müzik, video dosyaları) yüksek hacimli dosyaları göndermek veya indirmek kesinlikle yasaktır.

Tüm çalışanlar yaptıkları işler ve müşteriler ile ilgili bilgileri Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş.'den yazılı izin almadan; Sosyal Ağlar, Basın Yayın Organları ve başkaca kuruluşlar dahil hiçbir ortamda paylaşamazlar.

Çalışanlar hem Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş. veri tabanı üzerindeki bilgileri ve hem de hizmet verilen müşterilerin veri tabanları üzerindeki bilgileri korumak ve her ne sebep olursa olsun Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş.'nin yazılı izni alınmaksızın bu bilgilerin 3. Kişilerle paylaşılmamasını sağlamak için gerekli önlemleri almakla sorumludurlar.

Bütün kullanıcılar kendi bilgisayar sistemlerinin güvenliğinden sorumludurlar. Bilgisayarlarına yönelik her türlü saldırıyı fark ettikleri an zaman kaybetmeksizin yöneticilere bildirmekle sorumludurlar.

7.Yaptırımlar

Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, Avrupa Gayrimenkul Değerleme ve Danışmanlık A.Ş., Bilgi Güvenliği Politikası gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini uygulayabilir:

- Uyarma,
- Kınama,
- Para cezası,
- Sözleşme feshi.

8.Atıflar

İş Sürekliliği, Veri Yedekleme, Kalite Yönetim Prosedürleri bu politikayı destekler. Bu alanlarla ilgili işleyiş özel olarak dokümante edilmiş politika ve prosedürlerle tanımlanır.

9.Destek Politikalar

Erişim Denetim Politikası
Temiz Masa ve Temiz Ekran Politikası
E-mail Politikası
Taşınabilir Cihazlar Kullanım Politikası
Bilgi Güvenliği İhlal Olayı Politikası

10.Gözden Geçirme

Bu politika, Bilgi Güvenliği Ekibi tarafından periyodik olarak yılda bir gözden geçirilir. Yönetmeliklerde veya bilgi güvenliği uygulama süreçlerindeki değişiklikler politikanın gözden geçirilmesini gerektirir. Gözden geçirilen ve güncellenen politika üst yönetim tarafından onaylanır. Onaylanan politika AVRUPA web sayfasında yayınlanır.

11.Onay

AVRUPA yönetimi olarak, “Bilgi Güvenliği Yönetim Sistemi Politikası”nın uygulanmasının sağlanmasının ve kontrolünün yapılmasının, güvenlik ihlallerinde de gerekli yaptırımın icra edilmesinin yönetim tarafından desteklendiğini beyan ederim.

YÜRÜTME KURULU ÜYESİ

HAZIRLAYAN	ONAYLAYAN
BGYS SORUMLUSU	YÜRÜTME KURULU ÜYESİ