VERA KONSEPT GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.

BİLGİ SİSTEMLERİ YÖNETİMİ POLİTİKASI

1- AMAÇ VE KAPSAM

İşbu Bilgi Sistemleri Yönetimi Politikası ("**Politika**") **VERA KONSEPT GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.**'nin bilgi sistemlerinin ve bilgi varlıklarının; gizlilik, bütünlük, erişilebilirlik, doğruluk, süreklilik ve mevzuata uyum doğrultusunda yönetilmesine ilişkin temel esasları belirlemektir.

Bu Politika; bilgi sistemleri yönetimi süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların ve görev tanımlarının belirlenmesini, bilgi sistemleri hedeflerinin oluşturulmasını, bilgi sistemlerine ilişkin risklerin yönetilmesini, kontrollerin tesis edilmesini, değerlendirilmesini ve gözetimini kapsar.

Bu politika, Şirketimizin tüm birimlerini, çalışanlarını, yöneticilerini, bilgi sistemleri üzerinde yetkilendirilen kullanıcıları, Şirket adına bilgi sistemlerine erişim sağlayan üçüncü tarafları, dış hizmet sağlayıcıları, danışmanları ve Şirket'in sahip olduğu veya işlediği tüm bilgi varlıklarını kapsamaktadır. Çalışanlarımız (Kullanıcı) bu politikanın ekinde belirtilen kurallara, süreç ve talimatlara uymakla yükümlüdürler ve bu politikayı okuyarak işbu Politika'da tanımlanan kurallara uymayı taahhüt etmiş olurlar. Çalışanlarımıza, bilgi güvenliği farkındalığını artırmak amacıyla teknik ve davranışsal yetkinliklerini geliştirecek şekilde eğitimler gerçekleştirilecektir.

2- DAYANAK

Bu Politika, Sermaye Piyasası Kurulu'nun VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği başta olmak üzere ilgili sermaye piyasası mevzuatı, kişisel verilerin korunmasına ilişkin düzenlemeler, Şirket içi düzenlemeler ve Şirket'in faaliyet ölçeği ve ihtiyaçları ölçüsünde ISO 27001 standardı dikkate alınarak hazırlanmıştır.

3- GENEL İLKELER

3.1- Rol ve Sorumluluklar

Yönetim Kurulu ve Üst Yönetimin Sorumluluğu (Tebliğin m.7/1 ve 7/3 gereği) : Yönetim Kurulu, bilgi sistemleri kontrollerinin etkin, yeterli ve mevzuata uyumlu şekilde tesis edilmesi, değerlendirilmesi ve gözetilmesinden sorumludur. Bu Politika Yönetim Kurulu tarafından onaylanır.

Üst yönetim, bu Politika'nın uygulanmasını gözetir; bilgi sistemleri yönetimine ilişkin politika, prosedür ve süreçlerin oluşturulması, uygulanması, güncellenmesi ve ilgili taraflara duyurulması için gerekli mekanizmaları kurar. Üst yönetim ayrıca bilgi sistemleri risklerinin yönetilmesi, bilgi güvenliği ihlallerinin takip edilmesi, bilgi sistemleri

sürekliliğinin sağlanması ve çalışanlara gerekli eğitimlerin verilmesi için gerekli kaynakların tahsis edilmesini sağlar.

Bu Politika bakımından üst yönetim, Yönetim Kurulu tarafından belirlenen kişi veya grubu; böyle bir belirleme yapılmamışsa Şirket'in en üst yetkilisini ifade eder.

Bilgi Güvenliği Sorumlusu (Tebliğin m.7/5 gereği) : Bilgi Güvenliği Sorumlusu, bilgi sistemleri güvenliği kontrollerinin gereklerinin yerine getirilmesinden ve takibinden sorumlu, bilgi sistemleri güvenliğiyle ilgili riskleri ve bu risklerin yönetimini üst yönetime raporlayan kişidir. Bilgi Güvenliği Sorumlusu'nun bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda icrai/operasyonel bir görevinin bulunmaması ve üst yönetime bağlı çalışması esastır.

Bilgi Güvenliği Sorumlusu'nun bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi, kontrollerin tesisi veya bilgi güvenliği alanlarından herhangi birinde yeterli teknik bilgiye ve en az beş yıl tecrübeye sahip olması gözetilir.

Çalışanlar: Çalışanlar, kendilerine tahsis edilen bilgi sistemlerini ve bilgi varlıklarını yalnızca görevleri ve yetkileri kapsamında kullanmak; kullanıcı adı, parola ve benzeri kimlik doğrulama bilgilerini korumak; bilgi güvenliği ihlali veya şüphesi halinde belirlenen kanallar üzerinden bildirim yapmak ve Şirket tarafından duyurulan politika, prosedür, talimat ve kullanım kurallarına uymakla yükümlüdür.

Üçüncü Taraflar ve Dış Hizmet Sağlayıcılar: Şirket adına bilgi sistemlerine erişim sağlayan üçüncü taraflar ve dış hizmet sağlayıcılar, kendilerine bildirilen bilgi güvenliği kurallarına, gizlilik yükümlülüklerine, sözleşmesel düzenlemelere ve ilgili mevzuata uygun hareket etmekle yükümlüdür. Üçüncü taraflara verilecek erişimler, iş ihtiyacı ve en az yetki prensibi çerçevesinde sınırlandırılır.

3.2- Risk Yönetimi (Tebliğin m.8/1 ve 8/3 gereği)

Bilgi sistemlerine ilişkin risklerin yönetimi, Şirket'in genel risk yönetimi yaklaşımının bir parçasıdır. Şirket, bilgi sistemlerine ilişkin riskleri belirlemek, ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreç ve prosedürleri oluşturur. Bilgi sistemlerine ilişkin risk analizi yılda en az bir kez gerçekleştirilir; bilgi sistemlerinde, iş süreçlerinde veya dış hizmet yapısında önemli değişiklik olması halinde risk analizi yenilenir. Risk analizleri sonucunda tespit edilen iyileştirici faaliyetler, sorumluları ve hedef tarihleriyle birlikte kayıt altına alınır ve üst yönetime raporlanır.

Bilgi sistemleri yönetimine ilişkin politika, prosedür ve süreçlerin oluşturulması, uygulanması ve güncellenmesi üst yönetimin gözetiminde yürütülür. Bilgi Güvenliği Sorumlusu, bilgi sistemleri güvenliği kontrollerinin uygulanmasını takip eder ve bu kapsamdaki riskleri üst yönetime raporlar.

3.3- Bilgi Varlıkları Yönetimi

Şirket, sahip olduğu bilgi varlıklarını belirler, bunlara ilişkin envanter oluşturur ve söz konusu envanterin güncelliğini sağlar. Bilgi varlığı envanterinde asgari olarak varlığın tanımı, sahibi, kullanıcısı, konumu, güvenlik sınıfı ve yedekleme bilgisine yer verilir.

Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik gereksinimleri ile kritikliği ve hassasiyeti dikkate alınarak güvenlik sınıflandırması yapılır. Bilgi varlıklarının güvenlik sınıflarının belirlenmesine ilişkin esaslar yazılı hale getirilir ve üst yönetimin onayına sunulur.

Her bilgi varlığı için varlık sahibi belirlenir. Varlık sahibi, ilgili bilgi varlığının güvenlik gereksinimlerinin belirlenmesi, erişim yetkilerinin iş ihtiyacıyla uyumlu şekilde tanımlanması ve varlık envanterinin güncel tutulması süreçlerinde sorumluluk üstlenir.

Bilgi varlıklarının uygun kullanımına ilişkin usul ve esaslar Şirket tarafından yazılı hale getirilir, üst yönetim tarafından onaylanır ve ilgili personele duyurulur. Çalışanlar, kendilerine tahsis edilen bilgi sistemlerini ve bilgi varlıklarını yalnızca görevleri ve yetkileri kapsamında, mevzuata ve Şirket içi düzenlemelere uygun şekilde kullanmakla yükümlüdür.

Kullanımdan kaldırılan donanımsal bilgi varlıkları bakımından güvenli silme veya imha işlemleri uygulanır ve bu işlemler kayıt altına alınır. Kullanımdan kaldırılan yazılım ve uygulamalara ilişkin erişimler sonlandırılır; gerekli hallerde ilgili yazılım ve uygulamalar arşivlenerek sistemden kaldırılır.

Bu Politika kapsamında hizmet envanteri ve süreç envanterine ilişkin hususlar, Şirket'in tabi olduğu mevzuat hükümleri ve muafiyetler dikkate alınarak ayrıca değerlendirilir.

3.4- Erişim ve Yetkilendirme

Şirket bilgi sistemlerine erişimler, iş ihtiyacı, görevler ayrılığı ve en az yetki prensibi çerçevesinde tanımlanır. Kullanıcı hesabı açılması, yetkilendirme, yetki değişikliği, yetki iptali, görev değişikliği, işten ayrılma, ayrıcalıklı hesaplar ve uzaktan erişim süreçleri yazılı prosedürlere bağlanır. Erişim yetkileri düzenli olarak gözden geçirilir. Uzaktan erişimlerde güvenli bağlantı yöntemleri ve gerekli hallerde çok faktörlü kimlik doğrulama mekanizmaları kullanılır.

3.5- Dışarıdan Hizmet Alımı (Tebliğin m.19 gereği)

Şirket, bilgi sistemleri kapsamında dışarıdan hizmet alınması halinde, hizmet sağlayıcı seçimi öncesinde alınacak hizmetin niteliği, kritikliği, teknik yeterliliği, bilgi güvenliği riskleri ve hizmet sağlayıcının yeterliliği bakımından değerlendirme yapar. Kritik hizmetler bakımından değerlendirme sonuçları üst yönetimin onayına sunulur. Dış hizmet ilişkilerinde hizmet kapsamı, gizlilik, erişim, bilgi güvenliği yükümlülükleri, hizmet seviyesi, ihlal bildirimi, denetim ve sözleşmeye uygunluk hükümleri yazılı olarak belirlenir.

3.6- Bilgi Güvenliği İhlalleri ve Olay Yönetimi (Tebliğin m.24 gereği)

Şirket, bilgi güvenliği ihlallerinin, siber olayların, güvenlik açıklarının ve şüpheli faaliyetlerin bildirilmesi, değerlendirilmesi, sınıflandırılması, müdahale edilmesi, kayıt altına alınması ve raporlanmasına ilişkin süreçleri oluşturur. Çalışanlar ve üçüncü taraflar, bilgi güvenliği ihlali veya şüphesi halinde durumu derhal belirlenen iletişim kanalları üzerinden bildirmekle yükümlüdür.

3.7- Bilgi Sistemleri Sürekliliği ve Yedekleme

Şirket, kritik iş süreçlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olarak bilgi sistemleri süreklilik planı (Tebliğin m. 7/6 gereği) hazırlar. Yedekleme ihtiyaçları, bilgi varlıklarının kritikliği ve iş sürekliliği gereksinimleri dikkate alınarak belirlenir. Yedekleme ve yedekten geri dönüş süreçleri yazılı hale getirilir; plan ve test sonuçları yılda en az bir kez gözden geçirilerek üst yönetime raporlanır (Tebliğin m.27/8, m.27/12 ve m.27/13 gereği).

3.8- Eğitim ve Farkındalık

Şirket çalışanlarına bilgi güvenliği gereksinimleri, güncel tehditler, bilgi sistemleri kullanım kuralları, ihlal bildirim süreci ve rol/sorumlulukları hakkında yılda en az bir kez eğitim (Tebliğin m.7/3-ç ve m.9/5 gereği) verilmesi esastır. Eğitimlerin kapsamı çalışanların görev ve sorumluluklarına uygun şekilde belirlenir.

3.9- Politikanın Duyurulması (Tebliğin m.5/2 ve m.6/1 gereği)

Politika ve Politika kapsamında oluşturulan ilgili prosedür, talimat ve duyurular, kapsamına göre çalışanlara, ilgili üçüncü taraflara ve gerekli görülen diğer taraflara duyurulur. Politika'nın ilgili taraflara duyurulması amacıyla Şirket internet sitesinde yayımlanması da mümkündür.

4- GENEL KURALLAR

Çalışanlar, VERA KONSEPT GYO A.Ş.'nin Bilgi Güvenliği Yönetim Sistemi (BGYS) ISO 27001 Standardı gereği işbu Bilgi Güvenliği Politikası'na, VERA KONSEPT GYO A.Ş. Personel Yönetmeliği'ne, Disiplin Yönetmeliği'ne, Bilgi Güvenlik Politikasında atıf yapılan veya bahsi geçen tüm prosedürlere, talimatlara, mevzuata ve işbu taahhütname şartlarına uymayı, ve görevlerine ilişkin bilgi ve belgelerin gizliliğini korumayı taahhüt ederler. Her VERA KONSEPT GYO A.Ş. çalışanı bilgi gizliliğini korumakla sorumludur ve "**Personel Bilgilendirme Formu**'nu imzalar.

Şirket çalışanları, gerçekleştirdikleri çalışmalar sonucunda oluşturdukları her türlü bilgi, dosya ve/veya programın saklanması/muhafazası ve fiziksel güvenliğinin sağlanmasından sorumludurlar.

4.1- Elektronik Bilgiler:

• Şirket çalışanları kendi bilgisayarları üzerinde yer alan değerli ve kritik bilgilerinin Ortak Kullanım Sunucusu üzerinde güvenli olarak yedeklenmesinden sorumludurlar. Bu nedenle, çalışanlar tarafından işle ilgili değerli ve kritik bilgiler, kişisel bilgisayarlarda muhafaza edilmek yerine, Ortak Kullanım Sunucusu içinde çalışan için ayrılmış "Paylaşımlı" ve "Özel" isimli çalışma dosyalarında muhafaza edilecektir.

• Şirket tarafından tahsis edilmiş kişisel bilgisayarlar ve Ortak Kullanım Sunucusu üzerinde kullanıcının izni ve yetkisi dışındaki belge, bilgi veya yazılım alışverişinde bulunulmayacaktır.

• Yetkisi olmayan çalışanın, Şirket'in gizli ve hassas bilgilerini görmesi veya elde etmesi yasaktır. Bu nedenle, kişisel bilgisayarlar üzerinde problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmeyecektir ve karşılaşılan sorunlar yetkili kişilere bildirilecektir.

• Ortak Kullanım Alanların 'da gereksiz yer kaplayacak ve iş ile ilgili olmayan müzik ve resim dosyaları, oyunlar, filmler ve benzeri programların (mpg, mpeg, avi, exe, com, gif, jpg uzantılı dosyalar) bulundurulması yasaktır.

4.2- Kağıt Ortamındaki Bilgiler:

• Hassas olsun veya olmasın, çalışanların görevlerine ilişkin bilgi ve belgelerin gizliliği korunacak, bilgi ve belge niteliğindeki kâğıt ortamdaki dokümanlar, "**Back Up Kullanma Talimatı**"'na göre kayıt altına alınacaktır.

• Şirket çalışanları mesai saatleri dışında ve izinli olduğu dönemlerde masalarının üzerinde Şirkete ait hassas olsun olmasın hiçbir belgeyi açıkta bırakmayacaktır.

• Hassas bilgileri içeren kâğıt ve elektronik depolama ortamları kullanılmadığı zaman kilitli dolap ve/veya kasa içinde korunacaktır.

4.3- Bilgi ve Haberleşme Sistemleri ve Donanımları:

• İnternet, ortak kullanım sunucuları, e-posta, telefon, çağrı cihazları, faks, bilgisayarlar, mobil cihazlar ve cep telefonları da dahil olmak üzere Şirket Varlık Yönetimi Süreci uyarınca yönetilirler.

• Şirket telekomünikasyon cihazları kullanılırken ilgili yasa ve düzenlemelere uyulur.

• Şirket için veya Şirket adına alınmış olan, Şirket çalışanları veya ilgili kişiler tarafından Şirket için geliştirilmiş olan tüm donanımlar Şirket'in malıdır. Tüm donanımlar, ilgili lisans, uyarı, sözleşme ve anlaşmalar uyarınca kullanılacaktır.

• Şirketin bilgi ve haberleşme sistemleri ve donanımları öncelikli olarak Şirket işlerinin gerçekleştirilmesi için kullanılır. Şirket çıkarlarıyla çakışmadığı ve kullanım miktarları Şirketi maddi zarara uğratmayacak limitler dahilinde kullanıldığı sürece telekomünikasyon cihazlarının kişisel kullanımına izin verilir. Ancak, Şirketin normal

operasyon ve iş aktivitelerini engelleyemez. Kişisel kullanımlarda aşırılık tespit edildiği durumlarda Şirket telekomünikasyon cihazının kullanımını kısıtlama ve iptal hakkını saklı tutar.

• Kullanıcılar telekomünikasyon cihazları ile yaptıkları tüm iletişimden sorumludur.

• Şirket telekomünikasyon cihazlarını hiçbir şekilde yasa dışı kullanılamaz. Şirket telekomünikasyon cihazlarını uygunsuz içeriği saklamak, erişmek, indirmek ve iletmek için kullanılamaz. Kullanıcıların telekomünikasyon cihazlarını kullanmak için gerekli kimlik bilgilerini başkalarına vermeleri yasaktır. Ayrıca bilgi, zararlı yazılımlara karşı taramadan geçirilmeden Şirket ağına aktarılamaz.

• Bu sistemlerin yasa dışı, rahatsız edici, Şirketin diğer politika, standart ve rehberlerine aykırı veya Şirkete zarar verecek herhangi bir şekilde kullanımı, bu politikanın ihlal edildiği anlamına gelir.

5- PAROLA KULLANIMI VE UZAKTAN SİSTEME ERİŞİM KURALLARI

Şirket çalışanlarının gerçekleştirdikleri çalışmalar için kullanımlarına verilmiş masa üstü bilgisayarlar, notebooklar ve/veya mobil cihazlar üzerinden Şirket bilgisayar ağına erişmeleri sağlanmaktadır. Bilgi kaynaklarına erişim **“Şifre Talimatı”** ve **“Uzaktan Erişim Talimatı”’**na uygun olarak gerçekleştirilecektir.

• Uzaktan erişim, çalışanlara verilen “Kullanıcı Hesapları (User Account)” ile sağlanmaktadır.

• Sunucular ve ağ cihazları da dahil olmak üzere erişim kontrolünün sağlanması ve yetkisiz erişimin engellenmesi amacıyla her “Kullanıcı Hesabı” için kullanıcı adı ve parola verilmektedir.

• Her türlü kullanıcı şifresi çalışanın sorumluluğundadır.

• Çalışanlar kendilerine verilen kullanıcı adı ve parolaları kullanırken kendilerine duyurulan “Parola Kullanım ve Yönetim Talimatına uyacaklardır.

• Gerekmedikçe bilgisayar kaynakları paylaşıma açılmayacaktır, kaynakların paylaşıma açılması halinde de mutlaka “Parola Kullanım ve Yönetim Talimatı’ kurallarına göre hareket edilecektir.

• Çalışanlar, IT departmanı bilgisi dışında uzaktan erişimle bağlanamaz, bağlanırken ve bağlantıyı keserken bilgi verir, çalışırken işiyle ilgili olmayan dosyalara giremez. Yapılan uzaktan erişimlerin tamamı kayıt altında tutulacaktır.

• İnsan Kaynakları ile ilgili yazılımlara (PDKS), veri tabanına ve dosyalara İK’nın bilgisi ve izni dışında ulaşılamaz. İK ile ilgili yazılımlar ve veri tabanında ADMİN kullanıcı, İK Müdürü’dür. Loglar ise Bilgi İşlem Bölümü’ne açıktır.

• Kullanıcılar, kendilerine erişim izni verilmiş olan bilgiler ve alanlar dışındaki bilgi ve alanlara erişim girişiminde bulunmayacaklarını taahhüt etmişlerdir. Bu nedenle, yetkili olunmayan sunuculara erişilmesi; iç ve dış ağ güvenliğini veya ağ trafiğini bozacak eylemlere girişilmesi yasaktır.

• Şirkete, müşterilere, hizmet verilen diğer üçüncü taraflara ait olan her türlü bilginin açıklanması, çoğaltılması, değiştirilmesi, saptırılması, yok edilmesi, kaybedilmesi, amacı dışında kullanılması, çalınması veya yetkisiz olarak erişilmesi yasaktır.

6- İNTERNET KULLANIM KURALLARI

• Şirketin internet kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulur.

• Şirketin internet kaynakları öncelikli olarak Şirket işlerinin gerçekleştirilmesi için kullanılır. Şirket çıkarlarıyla çakışmayacak, Şirket'e zarar vermeyecek veya itibarını sarsmayacak şekilde internet kaynaklarının kişisel kullanımına izin verilmektedir.

• İnternet'ten temin edilecek ve iş için kullanılacak her bilginin güvenilirliğinden şüphe duyulmalı ve alınan bilginin eski ve hatalı olma olasılığı olduğu bilinmelidir.

• Kullanıcılar kişisel bilgisayarları ve/veya mobil cihazları üzerinden kendi kullanıcı hesaplarıyla internet üzerinde gerçekleştirilen tüm işlemlerden sorumludur. Bu nedenle kullanıcılar kullanıcı hesaplarını ve parolalarını uygun şekilde saklar ve başkaları ile paylaşamaz ve **"Şifre Talimatı"**'na uygun olarak değiştirir.

• İnternetten korsan yazılım, uygunsuz yazılı ve grafik malzemenin herhangi bir şekilde indirilmesi, kendisine ait olmayan parola, kendisine ait olmayan kredi kartı numaraları ile alışveriş yapılması kesinlikle yasaktır. Ayrıca, antivirüs programları, kırık programlar, ekran koruyucu, yamalar, masaüstü resimleri, yardımcı, tamir edici programlar gibi her türlü dosya ve programların indirilmesi ve/veya kurulması Bilgisayar İşletim Sistemleri'ne zarar verdiği için yasaktır.

• Şirket malı sayılan, Şirket iç kullanımı için hazırlanmış, Şirket'in müşterileri ile ilişkilerini veya Şirket imajını etkileyecek, Şirket tarafından onaylanmamış, her türlü bilgi, belge, dosya, duyuru ve/veya yazılımın (iş potansiyelleri, birim maliyetleri, fiyatlar, yatırımlar, ihale bilgileri vb.), Şirket tarafından verilen görevler dışında kullanımı ve dağıtılması, internet üzerinden satılması, açıklanması, kiralanması ve/veya başkaca bir yöntem ile Şirket dışındaki üçüncü kişilere herhangi bir nedenle iletilmesi kesinlikle yasaktır. Şirket'e ait önemli bilgilerin yetkisiz kişilere verildiği veya açıklandığı belirlendiğinde veya bu konuda şüphe oluştuğu durumda, **İnsan Kaynakları Yönetmeliği** ve **Disiplin Süreci** uygulanır.

• Şirket kaynakları, uygunsuz içeriği saklamak, bağlantı olarak vermek, yer imi olarak eklemek, erişmek ve göndermek için kullanılamaz.

7- YAZILIM KULLANIM VE FİKRİ MÜLKİYET HAKLARINA UYUM KURALLARI

Şirket bilgisayarlarına kurulan yazılımlar **“Şirket Varlık Yönetimi Süreci”** uyarınca yönetilirler.

• Şirkete ait yazılımlar kullanılırken ilgili yasa ve düzenlemelere uyulacaktır.

• Yazılımlar ilgili lisans, uyarı, kontrat ve anlaşmalar uyarınca kullanılacaktır.

• Şirket için veya Şirket adına kullanım hakkı alınmış olan, Şirket çalışanları veya Şirket için geliştirilmiş olan tüm yazılımlar Şirket varlık envanterine kayıtlı olup Şirket malıdır.

• Kullanım haklarının ihlalinin önlenmesi için yazılımlar Şirket tarafından güvenilir kaynaklardan ve Satınalma Süreçlerine uygun olarak sağlanacaktır.

• Şirketin internet kaynakları ve haberleşme alt yapısı, onaylanmamış, ücretsiz ticari hiçbir yazılım için kullanılamaz. Şirket izni olmadan ticari hiçbir yazılım kopyalanamaz, gönderilemez, alınamaz veya çoğaltılamaz.

• Yazılım ve diğer ürünler için, yalnız lisanslı sürümlerin lisans adetleri dahilinde kullanıldığı, Şirket tarafından yapılacak kontrollerle denetlenecektir.

• Lisans veya sözleşmelerinde aksi belirtilmediği sürece yazılımların, yedekleme ve arşivleme dışında, herhangi bir şekilde kopyalanması ilgili Mevzuata göre suçtur. Kanunlarca yasaklanmasının yanı sıra, izinsiz yazılım kopyalanması işbu Politikanın ihlal edilmesi anlamına gelmektedir.

8- ANTİ-VİRÜS POLİTİKASI

• Şirket bilgisayarlarında lisanslı anti-virüs yazılımı yüklenir ve daimi çalışmaları sağlanır.

• Anti-virüs yazılımı yüklü olmayan bilgisayarların, kullanıma açılması ve Şirket ağına bağlanmaları yasaktır. Antivirüs yazılımı yüklü olmayan bilgisayarlar tespit edildiğinde, Şirket’in ilgili birimine haber verilecektir.

• Hiçbir kullanıcı anti-virüs yazılımını kullandığı sistemden kaldıramaz ve başka anti-virüs yazılımını sistemine kuramaz.

• Zararlı virüs programlarını (örneğin; virüsler, solucanlar, truva atı, e-posta bombaları vb.) Şirket bünyesinde oluşturmak ve dağıtmak yasaktır.

• Antivirüs yazılımı kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse anti-virüs programları ile yeni nesil virüslere karşı korunmalıdır.

9- ELEKTRONİK POSTA KULLANIM KURALLARI

• Şirket e-posta kaynakları kullanılırken ilgili yasa ve düzenlemelere uyulur. Şirket e-posta kaynakları öncelikli olarak resmi ve onaylı Şirket işlerinin gerçekleştirilmesi için kullanılacaktır.

1. Şirket çalışanları tanımlanan görevlerinin yerine getirilmesinde kendilerine sağlanacak şirket kaynaklarını kullanarak elektronik posta gönderecek / alacaklardır.

2. Şirket çalışanları kendi kullanıcı hesaplarıyla gerçekleştirilen tüm e-posta işlemlerinden sorumludur.

3. Şirket çalışanları kendi yetki alanlarındaki kurumsal elektronik postaların yetkisiz kişiler tarafından görünmesi ve okunmasını engellemekten sorumludurlar.

4. E-posta sistemlerinde parola kullanılır. Kişisel parolalar, Şirketin yetkili sorumluları dahil üçüncü kişilere gösterilemez veya başkalarıyla paylaşılamaz. Aksi durumlarda, parolasını paylaşan kişi parolayı öğrenen kişinin kendisi adına yapacaklarının sorumluluğunu kabul etmiş sayılır. Kişisel parolalar, çalışanın iş sözleşmesinin sonlandırılması ve acil durumlarda Admin Yetkili Sorumlu tarafından iptal edilir.

5. Elektronik posta erişimi için kullanılan donanım/yazılım sistemleri yetkisiz erişimlere karşı korunur.

• Şirket çalışanları elektronik postalarını düzenli olarak kontrol etmelidir.

1. E-postalar mümkün olan en kısa sürede yanıtlanacak veya ilgili kişiye yönlendirilecektir.

2. E-posta eklentileri kritik ve değerli olan dokümanlar **“Sunucu Güvenlik Talimatı”** ‘na uygun şekilde arşivlenecektir.

3. “Konu” kısmında “Duyuru” yazmasa bile “Kime” kısmında çok kullanıcıyı içeren **Duyuru amaçlı e-postaların gönderilme yetkisi İnsan Kaynakları Departmanı’ndadır.** Duyuru amacıyla gönderilecek olan e-postalar İnsan Kaynakları Müdürü’nün kontrolünden sonra, İnsan Kaynakları Müdürü tarafından ilgililere duyurulur.

4. Şirket dışına gönderilen tüm e-postalarda aşağıdaki uyarı mesajı bulunacaktır:

“Bu e-posta mesajı ve ekleri gönderildiği kişi ya da kuruma özeldir ve gizlidir. Ayrıca hukuken de gizli olabilir. Hiçbir şekilde üçüncü kişilere açıklanamaz ve yayınlanamaz. Eğer mesajın gönderildiği alıcı değilseniz bu elektronik postanın içeriğini açıklamanız, kopyalamanız, yönlendirmeniz ve kullanmanız kesinlikle yasaktır ve bu elektronik postayı ve eklerini derhal silmeniz gerekmektedir. VERA KONSEPT GYO A.Ş. bu mesajın içerdiği bilgilerin doğruluğu veya eksiksiz olduğu konusunda herhangi bir garanti vermemektedir. Bu nedenle bu bilgilerin ne şekilde olursa olsun içeriğinden, iletilmesinden, alınmasından, saklanmasından ve kullanılmasından sorumlu değildir. Bu mesajdaki görüşler gönderen kişiye ait olup, VERA KONSEPT GYO A.Ş.’nin görüşlerini yansıtmayabilir.

This e-mail and its attachments are private and confidential and intended for the exclusive use of the individual or entity to whom it is addressed. It may also be legally confidential. Any disclosure, distribution or other dissemination of this message to any third party is strictly prohibited. If you are not the intended recipient you are hereby notified that any dissemination, forwarding, copying or use of any of the information is strictly prohibited, and the e-mail should immediately be deleted. VERA KONSEPT GYO A.Ş. makes no warranty as to the accuracy or completeness of any information contained in this message and hereby excludes

any liability of any kind for the information contained therein or for the transmission, reception, storage or use of such information in any way whatsoever. The opinions expressed in this message are those of the sender and may not necessarily reflect the opinions of VERA KONSEPT GYO A.Ş. ”

• Şirket çalışanlarının elektronik posta kullanımında ahlaki kurallara ve yürürlükteki mevzuata uygun hareket etmeleri zorunludur.

1. Şirket çıkarlarıyla çatışmadığı sürece ve sistemi gereksiz meşgul edecek büyüklükte olmamasına dikkat etmek şartı ile e-posta kaynaklarının kişisel kullanımına izin verilmektedir.

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

3. Kişisel kullanım için İnternet’teki listelere üye olunması durumunda Şirket elektronik posta adresleri kullanılmaz.

4. Şirket elektronik posta sistemi, taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kesinlikle kullanılamaz.

5. Şirketin e-posta sistemi ücretsiz veya ticari hiçbir yazılımın alınması, Bilgi işlem bölümü bilgisi haricinde gönderilmesi veya saklanması için kullanılamaz.

6. Kullanıcıların bilgi paylaşımını elektronik posta yönlendirme, dosya sunucuları ve diğer yetkilendirilebilir Bilgi Güvenliğinin belirlemiş olduğu mekanizmalarını kullanarak yapmaları gerekir.

7. Şirket çalışanları dışında sistem üzerinde elektronik posta kutusu yaratılmaz.

• Kullanıcılar gereksiz elektronik postaları silmekle yükümlüdür.

1. Elektronik postalar virüs, elektronik posta bombaları ve Truva atı gibi zararlı kodlar içerebilirler.

2. Kaynağı bilinmeyen elektronik postalar ve ekinde gelen dosyalar; zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren elektronik postalar; kullanıcı

kodu/parolasını girmesini isteyen elektronik postalar herhangi bir işlem yapılmaksızın Bilgi İşlem Departmanı'na bilgi verilecek; kesinlikle açılmayacak, yanıt yazılmayacak ve derhal silinecektir ve kesinlikle başkalarına iletilmeyecektir.

• E-posta Yazılımı

1. Kullanıcılar sadece Şirketin yetkili birimlerince onaylanmış e-posta yazılımlarını ve konfigürasyonlarını kullanabilirler.

2. E-posta yazılımının mevcut güvenlik ayarlarını değiştirmek yasaktır.

3. Kullanıcılar e-posta yazılımında gönderen kimliğini gizleyecek özelliklerini kullanmaları yasaktır.

• Şirket kullanıcıları için elektronik posta hesabı alımı ve kullanımı, kullanımdan kaldırılması, İnsan Kaynakları departmanı bilgilendirilmesi ile Bilgi Teknolojileri Yöneticisi tarafından yönetilir.

• Tüm elektronik posta sistemleri ve bu sistemler üzerinde yaratılan, tutulan ve/veya saklanan mesaj, bilgi ve dosyaların hepsi (yedeklenen kopyaları dahil) Şirket bilgi varlığı olarak kabul edilmektedir.

• Güvenliğinden emin olunmayan bilgisayarlardan (örneğin internet cafe gibi ortak kullanım alanındaki bilgisayarlar) web e-posta sistemi kullanılamaz.

10- İZLEME VE DENETLEME HAKLARI

Şirket, bilgi sistemlerinin güvenliği, mevzuata uyum, iş sürekliliği ve Şirket içi düzenlemelerin uygulanması amacıyla bilgi sistemleri kullanımına ilişkin denetim izi kayıtlarını ilgili mevzuata uygun şekilde tutabilir, izleyebilir ve inceleyebilir. Bu kapsamda elde edilen kayıtlar yalnızca yetkili kişiler tarafından, meşru amaçlarla ve ilgili mevzuata uygun olarak işlenir; yetkili kamu kurum ve kuruluşlarıyla ancak mevzuatın gerektirdiği hallerde paylaşılır.

11- UYGULAMA VE YAPTIRIMLAR

Bu Politika'ya ve bu Politika kapsamında yayımlanan prosedür, talimat ve duyurulara aykırı hareket edenler hakkında, ihlalin niteliğine göre ilgili mevzuat, iş sözleşmeleri ve Şirket içi disiplin düzenlemeleri çerçevesinde gerekli işlemler uygulanır. Gerekli görülen hallerde hukuki ve cezai yollara başvurulabilir.

12- YÜRÜRLÜK

İşbu Politika, Şirket Yönetim Kurulu'nun **22/06/2026** tarihli ve **2026-16** sayılı kararı ile yürürlüğe girer. Politika yılda en az bir kez veya mevzuat, organizasyon yapısı, iş süreçleri, teknoloji altyapısı ya da risklerde önemli değişiklik olması halinde gözden geçirilir ve gerekli hallerde güncellenerek Yönetim Kurulu onayına sunulur.