BERA HOLDİNG A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

1. KAPSAM

Bera Holding A.Ş.'nin stratejik hedeflerinin desteklenmesi, sahip olduğu marka değerinin korunması ve yürürlükteki yasal düzenlemeler ile uyumun sağlanması amacıyla; bilgi güvenliğine ilişkin temel kuralların ve prensiplerin belirlenmesi, bilgi güvenliği süreçlerinin etkin şekilde işletilmesi ile bu süreçlere ilişkin rol ve sorumlulukların tanımlanması bu Politika'nın temel çerçevesini oluşturmaktadır.

Şirket mülkiyetinde bulunan her türlü bilgi ve bilgi varlığı bu Politika kapsamına dâhil olup, Bera Holding bünyesinde yürütülen tüm faaliyetler ile işletilen iş süreçlerinin, bilgi güvenliği gereklilikleri gözetilerek ve bu Politika hükümlerine uygun şekilde gerçekleştirilmesi esastır.

2. AMAÇ VE YASAL DAYANAK

Şirket bilgi varlıklarının siber tehditlere karşı korunmasını teminen; politika, prosedür, organizasyon yapısı ve teknik kontrolleri kapsayan **Bilgi Güvenliği Yönetim Sistemi (BGYS)** oluşturulmuştur. BGYS'nin temel amacı; bilgilerin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlamak, bilgilerin doğruluğunu ve bütünlüğünü korumak, aynı zamanda bilgi ve bilgi sistemlerinin ihtiyaç duyulduğunda kesintisiz şekilde kullanılabilir olmasını temin etmektir.

Bilgi Güvenliği Yönetim Sistemi; bilgi güvenliği stratejisinin belirlenmesi, güvenlik politikalarının oluşturulması ve uygulanması, güvenlik altyapılarının kurulması, işletilmesi, izlenmesi ve sürekli geliştirilmesine yönelik süreç ve operasyonları kapsamaktadır. Bilgi Güvenliği Politikası ise, halka açık şirketler için Sermaye Piyasası Kurulu tarafından yürürlüğe konulan **VII-128.9 Bilgi Sistemleri Yönetimi Tebliği** ile **6698 sayılı Kişisel Verilerin Korunması Kanunu** başta olmak üzere ilgili mevzuat dikkate alınarak hazırlanmıştır.

Şirket, bilgi güvenliği kapsamında aşağıda belirtilen hususların yerine getirilmesini temel ilke olarak benimser:

- Bilgi varlıklarını sistematik biçimde yönetmek; varlıkların güvenlik değerlerini, ihtiyaçlarını ve maruz kalabilecekleri riskleri belirlemek, bu risklere yönelik uygun kontrolleri geliştirmek ve uygulamak,
- Bilgi varlıkları, bu varlıkların değerleri, güvenlik gereksinimleri, zafiyetleri ile varlıklara yönelik tehditlerin ve tehditlerin gerçekleşme sıklıklarının belirlenmesine ilişkin çerçeveyi tanımlamak,
- Tehditlerin bilgi varlıkları üzerindeki gizlilik, bütünlük ve erişilebilirlik etkilerini değerlendirmeye yönelik risk analiz yaklaşımını oluşturmak,
- Bilgi güvenliği risklerinin ele alınmasına ve yönetilmesine ilişkin çalışma esaslarını ortaya koymak,
- Hizmet verilen kapsam doğrultusunda teknolojik gelişmeleri ve beklentileri düzenli olarak gözden geçirerek bilgi güvenliği risklerini sürekli izlemek,

- Tabi olunan ulusal ve uluslararası düzenlemelerden, yasal mevzuattan, sözleşmelerden ve kurumsal sorumluluklardan kaynaklanan bilgi güvenliği gereksinimlerini karşılamak,
- Hizmet sürekliliğini tehdit edebilecek bilgi güvenliği risklerinin etkisini azaltmak ve iş sürekliliğine katkıda bulunmak,
- Gerçekleşebilecek bilgi güvenliği olaylarına hızlı ve etkin şekilde müdahale edebilecek yetkinlik ve organizasyonel yapıyı tesis etmek,
- Maliyet etkin bir kontrol altyapısı oluşturarak bilgi güvenliği seviyesini korumak ve zaman içinde geliştirmek,
- Kurum itibarını güçlendirmek ve bilgi güvenliği kaynaklı olumsuz etkilerden kurumu korumak,
- Bilgi Güvenliği Yönetim Sistemi'nin sürekliliğini sağlamak,
- Bilgi Güvenliği Yönetim Sistemi'nin sürekli iyileştirilmesine yönelik tüm çalışmaları desteklemek.

3. YÖNETİM

Yönetim Kurulu

Bilgi Güvenliği Politikası, Üst Yönetim tarafından hazırlanır ve Yönetim Kurulu onayı ile yürürlüğe girer. Bilgi güvenliği kapsamında bilgi sistemleri üzerinde etkin, yeterli ve sürdürülebilir kontrollerin tesis edilmesi ve gözetilmesi Yönetim Kurulu'nun nihai sorumluluğundadır. Yönetim Kurulu, politikanın uygulanmasının gözetimi amacıyla Üst Yönetimi yetkilendirir. Yetki ve sorumlulukların belirlenmesinde görevler ayrılığı ilkesine uyum esastır.

Üst Yönetim

Üst Yönetim; bilgi güvenliğine ilişkin kurumsal yönetim çerçevesinin oluşturulmasından, sürdürülmesinden ve Bilgi Güvenliği Politikası'nın yaşayan bir doküman olarak güncel tutulmasından sorumludur. Bu kapsamda politika; Şirket ve iştiraklerinin faaliyetlerine, iş gerekliliklerine, bilgi varlıklarına ve bilgi sistemlerinin maruz kaldığı risk ve tehdit ortamındaki değişikliklere uyum sağlayacak şekilde düzenli olarak gözden geçirilir.

Bilgi Güvenliği Politikası kapsamında hazırlanması gereken standart, prosedür ve talimatların onaylanmasına ilişkin yetki, Yönetim Kurulu tarafından **Mali İşler Direktörlüğü'nün temsil edildiği Üst Yönetim** yapısına verilmiştir.

Bilgi güvenliği politikasının uygulanması Üst Yönetim tarafından gözetilir. Üst Yönetim; bilgi güvenliği önlemlerinin yeterli ve etkin seviyede tesis edilmesi konusunda gerekli iradeyi ortaya koyar, bu amaçla yürütülecek faaliyetler için yeterli insan kaynağı, teknik altyapı ve finansal kaynağın tahsisini sağlar. Ayrıca bilgi sistemleri ve bu sistemler üzerinde işlenen, iletilen ve saklanan verilerin gizlilik, bütünlük ve erişilebilirliğini temin edecek kontrollerin geliştirilmesini, işletilmesini ve güncel tutulmasını sağlar; bu kapsamda gerekli yönetsel sorumlulukları tanımlar.

Üst Yönetim'in gözetim ve sorumlulukları aşağıda belirtilmiştir:

- Bilgi güvenliği politikalarının, tanımlı rollerin ve sorumlulukların en az yılda bir kez gözden geçirilmesi ve onaylanması,

- Bilgi sistemleri ve iş süreçlerine ilişkin potansiyel risklerin, etkileriyle birlikte tespit edilmesi ve bu risklerin azaltılmasına yönelik faaliyetleri içeren risk yönetimi sürecinin işletilmesi,
- Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi, analiz edilmesi ve sonuçlarının periyodik olarak değerlendirilmesi,
- Çalışanların bilgi güvenliği farkındalığını artırmaya yönelik eğitim ve bilinçlendirme faaliyetlerinin planlanması ve uygulanması,
- Bilgi sistemlerine ilişkin risklerin yönetilmesi amacıyla oluşturulan süreç ve prosedürlerin, organizasyonel ve yönetsel yapı içerisinde fiilen uygulanmasının sağlanması ve etkinliğinin izlenmesi,
- Bilgi sistemleri güvenliğine ilişkin süreç ve kontrollerin uygulanmasından ve izlenmesinden sorumlu, bilgi güvenliği riskleri ve bu risklerin yönetimine ilişkin olarak Üst Yönetim'e düzenli raporlama yapan, yeterli teknik bilgi ve deneyime sahip bir **Bilgi Sistemleri Güvenliği Sorumlusu'nun** atanması,
- Risk öncelikleri dikkate alınarak kritik iş süreçlerinin sürekliliğinin sağlanması amacıyla iş sürekliliği ve felaket kurtarma planlarının hazırlanması; bu planlarda kabul edilebilir azami kesinti süreleri ve veri kaybı seviyelerinin belirlenmesi,
- Bilgi güvenliği ile ilgili önemli gelişmelerin ve kritik risklerin gerekli görülen durumlarda Yönetim Kurulu'na raporlanması.

4. SORUMLULUKLAR

Bilgi Sistemleri Güvenliği Sorumlusu

Bilgi Sistemleri Güvenliği Sorumlusu; bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin uygulanmasından, izlenmesinden ve etkinliğinin sağlanmasından sorumlu olan; bilgi sistemleri güvenliğiyle ilgili riskleri ve bu risklerin yönetimine ilişkin hususları Üst Yönetim'e düzenli olarak raporlayan, yeterli teknik bilgi ve deneyime sahip kişidir. Bu kapsamda Bilgi Sistemleri Güvenliği Sorumlusu; bilgi güvenliği olaylarının ele alınmasında rehberlik eder, Politika'nın detaylı standartlar, prosedürler ve süreçlerle desteklenmesini sağlar ve bu dokümanların gerektiğinde kullanıma hazır olmasını temin eder.

Bilgi Güvenliği Politikasının, ilgili tüm standartların, destekleyici dokümanların ve farkındalık eğitimlerinin işlevsel sahipliği Bilgi Sistemleri Güvenliği Sorumlusu tarafından yürütülür. Bu görev aynı zamanda Politika'nın Şirket genelinde uygulanmasına ilişkin danışmanlık ve rehberlik fonksiyonunu da kapsar. Politika hükümlerinin tüm çalışanlara (daimî, dönemsel, sözleşmeli) ve yüklenici personeline duyurulması ve benimsetilmesi de Bilgi Sistemleri Güvenliği Sorumlusu'nun sorumluluğundadır.

Bilgi Sistemleri Güvenliği Sorumlusu'nun başlıca sorumlulukları aşağıda yer almaktadır:

- Bilgi güvenliği farkındalık eğitimlerinin etkinliğini ölçmek, değerlendirmek ve sonuçlarını raporlamak,
- Şirket Bilgi Güvenliği Politikası, standartları ve prosedürlerini periyodik olarak gözden geçirmek ve gerekli güncellemeler için öneriler geliştirmek,
- Bilgi güvenliği zafiyetleri ve olaylarının nedenlerini araştırmak; gerekli durumlarda delillerin korunmasını sağlamak ve iyileştirici/önleyici tedbirler önermek,
- Belirlenmiş kritik güvenlik kontrollerinin uygulanmasını ve sürekliliğini sağlamak,

- İş sürekliliği ve felaket kurtarma planlarının işletildiğini, test edildiğini ve denetlendiğini izlemek,
- Bilgi güvenliği ile ilgili iç ve dış otoriteler, çalışma grupları ve paydaşlar ile iletişim ve koordinasyonu sağlamak,
- Gerekli durumlarda bilgi sistemleri güvenliği konularında Şirket'i dış paydaşlar nezdinde temsil etmek,
- Bilgi sistemleri güvenliğine ilişkin riskler ve bu risklerin yönetimi konusunda Üst Yönetim'e düzenli raporlama yapmak.

Kurum Personelinin Sorumlulukları

Şirket bünyesinde görev yapan tüm çalışanlar; Bilgi Güvenliği Yönetim Sistemi kapsamında yayımlanmış politika, prosedür ve talimatlara uymakla, gerçekleşmiş veya gerçekleşmesi muhtemel bilgi güvenliği ihlallerini ve zafiyetlerini bildirmekle ve Şirket tarafından talep edilen bilgi güvenliği faaliyetlerini yerine getirmekle yükümlüdür.

Çalışanlar, görev ve pozisyonları ne olursa olsun, işlerini Şirket bilgi ve bilgi varlıklarının korunmasını gözeterek yürütmekle sorumludur. Bilgi Güvenliği Politikası hükümleri; tam zamanlı, yarı zamanlı, daimî veya sözleşmeli tüm personel için, coğrafi konum veya organizasyon biriminden bağımsız olarak bağlayıcıdır.

Bu çerçevede **Varlık ve Süreç Sahiplerinin** sorumlulukları aşağıda belirtilmiştir:

- Kendilerine duyurulan Bilgi Güvenliği Politikası ve ilgili prosedürlere uymak,
- Sorumlu oldukları süreç ve sistemlere ilişkin oluşturulan dokümanlarda (süreç, akış, talimat, kılavuz, form vb.) bilgi güvenliği dokümanlarıyla uyumu sağlamak,
- Bilgi güvenliği politika ve prosedürlerine uyumsuzlukları veya bilgi güvenliği ihlal olaylarını ilgili bildirim kanalları üzerinden Bilgi Sistemleri Güvenliği Sorumlusu'na iletmek,
- Bilgi sistemlerinin çalışmasını olumsuz etkileyecek veya bilgi güvenliğini riske atabilecek faaliyetlerden kaçınmak,
- Bilgi güvenliği dokümanlarına ilişkin güncelleme ve iyileştirme taleplerini Bilgi Sistemleri Güvenliği Sorumlusu'na bildirmek,
- Bilgi ve kurumsal kaynaklara yalnızca iş ihtiyaçları ölçüsünde erişim talep etmek,
- Sahibi oldukları varlıklar ve kişisel veriler için erişim yetkilerini, kullanıcı ve yönetici ayrıcalıklarını belirlemek ve güncelliğini sağlamak,
- Sorumluluk alanlarındaki varlık envanterlerinin doğruluğunu ve güncelliğini takip etmek.

Bilgi Güvenliği Politikası hükümleri, Şirket İnsan Kaynakları düzenlemeleri ve personel yönetmeliği ile uyumlu şekilde uygulanır. Her çalışan, Politika'dan haberdar olmak ve bu ilkelere uygun hareket etmekle yükümlüdür. Çalışanlar, Politika'nın geliştirilmesine yönelik önerilerini Bilgi Sistemleri Güvenliği Sorumlusu'na iletebilir; bu öneriler değerlendirilerek gerekli görülen durumlarda Politika güncellenir.

Üçüncü Tarafların Sorumlulukları

Şirket'e mal veya hizmet sağlayan üçüncü taraflar ile bunların çalışanlarının uyması gereken bilgi güvenliği yükümlülükleri; ilgili sözleşmeler, protokoller ve güvenlik taahhütleri ile belirlenir. Üçüncü taraflar, asgari olarak aşağıdaki hususlara uymakla yükümlüdür:

- Şirket ile yapılan sözleşme ve protokoller kapsamında bildirilen bilgi güvenliği kurallarına ve ilgili Şirket politika ve prosedürlerine uygun hareket etmek,
- Şirket'e ait bilgi ve bilgi varlıklarını, Şirket'in yazılı onayı olmaksızın üçüncü kişilerle paylaşmamak,
- Kendilerine tahsis edilen kimlik, kullanıcı hesapları ve erişim yetkilerini sözleşme ve talimatlara uygun şekilde kullanmak,
- Şirket'in onayı olmadan Şirket sistemlerindeki veri ve yazılımları kopyalamamak; ses, görüntü veya veri kaydı almamak ve bilgi güvenliğini veya kurumsal itibarı zedeleyebilecek herhangi bir faaliyette bulunmamak,
- Şirket lokasyonlarında gerçekleştirilecek sistem erişimlerini Bilgi Teknolojileri birimlerinin gözetiminde gerçekleştirmek.

Şirket personeli statüsünde olmayan ancak Şirket bilgilerine erişim ihtiyacı bulunan tüm üçüncü taraf hizmet sağlayıcılar ve destek personeli; bu Politika'nın genel ilkelerine ve kendileri için tanımlanmış bilgi güvenliği yükümlülüklerine uymakla yükümlüdür.

5. DENETİM VE KONTROL

Şirket, bilgi sistemlerine ilişkin risklerin etkin bir şekilde yönetilmesini teminen; risklerin tanımlanması, analiz edilmesi, ölçülmesi, izlenmesi, işlenmesi ve raporlanmasına yönelik denetim ve kontrol mekanizmalarını tesis eder ve bu mekanizmaların güncelliğini sağlar. Bilgi sistemlerine ilişkin risk analizi, risk işleme ve gözetim faaliyetleri tanımlı süreçler çerçevesinde yürütülür.

Bu kapsamda;

- Bilgi sistemlerine ilişkin risk analizi en az yılda bir kez gerçekleştirilir,
- Bilgi sistemleri altyapısı, uygulamalar, iş süreçleri veya organizasyonel yapıda meydana gelen önemli değişiklikler sonrasında risk analizi yeniden yapılır,
- Risk analizi çalışmalarında tüm bilgi varlıkları değerlendirmeye alınır ve varlıkların gizlilik, bütünlük ve erişilebilirlik boyutları esas alınır,
- Risklerin kabulü, azaltılması, devri veya kaçınılmasına yönelik kararlar tanımlı risk işleme yöntemleri çerçevesinde ele alınır.

Bilgi sistemleri süreçleri ve bu süreçlere ilişkin kontrollerin etkinliği, yeterliliği ve mevzuata uyumu düzenli olarak izlenir ve değerlendirilir. Ayrıca öngörülen risklerin veya gerçekleşen risklerin etkisini azaltmaya yönelik faaliyetlerin durumu sürekli takip edilir. Bu doğrultuda;

- Tespit edilen önemli kontrol eksiklikleri ve iyileştirme alanları kayıt altına alınır,
- Uygulanan düzeltici ve önleyici faaliyetlerin sonuçları izlenir ve değerlendirilir,

- Önemli bulgular ve gerçekleştirilen çalışmalar en az yılda bir kez Üst Yönetim'e raporlanır ve gerekli aksiyonların alınması sağlanır.

Bilgi Güvenliği Politikası'nın, bu politika kapsamında oluşturulan tüm standartların, prosedürlerin, destekleyici dokümanların ve farkındalık/eğitim faaliyetlerinin işlevsel sahipliği **Bilgi Sistemleri Güvenliği Sorumlusu** tarafından yürütülür. Bu görev, aynı zamanda Politika'nın Şirket genelinde etkin biçimde uygulanmasına yönelik danışmanlık ve rehberlik rolünü de kapsar.

Her birim yöneticisi; sorumluluk alanı dâhilinde Bilgi Güvenliği Politikası'na uyumun sağlanması için gerekli idari ve teknik tedbirleri almak, ilgili kontrollerin uygulanmasını gözetmek ve sistemin işleyişini izlemekten birinci derecede sorumludur.

Bilgi Güvenliği Politikası hükümlerine aykırı davranılması; Şirket'in bilgi varlıklarının zarar görmesine, güvenlik risklerinin artmasına ve yasal yükümlülüklerin ihlal edilmesine neden olabilir. Bu kapsamda;

- Politika ihlalleri, Şirket açısından operasyonel, finansal ve itibar riskleri doğurabilir,
- İhlalin niteliğine göre, yürürlükteki mevzuat kapsamında idari, hukuki ve cezai sorumluluklar gündeme gelebilir,
- Bilgi Güvenliği Politikası ihlalleri, aynı zamanda Şirket Personel Yönetmeliği kapsamında disiplin ihlali sayılır,
- Gözetim, denetim veya ihbar yoluyla tespit edilen ihlaller; disiplin cezalarının uygulanması, iş sözleşmesinin feshi ve gerekli görülen durumlarda adli ve cezai süreçlerin başlatılması ile sonuçlanabilir.

6. HEDEFLER

Bera Holding A.Ş.'nin Bilgi Güvenliği Yönetimi; Şirket'in kurumsal itibarının ve güvenilirliğinin korunması, bilgi varlıklarının güvence altına alınması ve temel ile destekleyici iş faaliyetlerinin mümkün olan en düşük kesinti ile sürdürülebilmesi hedefleri doğrultusunda yapılandırılmıştır. Bu kapsamda bilgi güvenliği hedefleri aşağıda belirtilmiştir:

- Bilgi sistemlerinin sürekliliğini ve erişilebilirliğini sağlayarak kritik iş süreçlerinin kesintisiz şekilde yürütülmesini temin etmek,
- Bilgi güvenliği kontrollerinin etkinliğini artırmak suretiyle çalışanların farkındalık düzeyini yükseltmek ve tanımlı güvenlik gereksinimlerine uyumu en üst seviyeye çıkarmak,
- Üçüncü taraflar ile gerçekleştirilen iş ilişkilerinde, sözleşmeler ve güvenlik taahhütleri kapsamında belirlenen bilgi güvenliği yükümlülüklerine tam uyumu sağlamak,
- Bilgi güvenliği ihlallerinin gerçekleşme olasılığını en aza indirmek; meydana gelen olayları analiz ederek kurumsal öğrenme ve sürekli iyileştirme fırsatına dönüştürmek,
- Bilginin üretilmesi, işlenmesi, iletilmesi ve saklanması süreçlerinin yürürlükteki mevzuata, yasal düzenlemelere ve sözleşmesel yükümlülüklere tam uyumlu şekilde gerçekleştirilmesini sağlamak,
- Bilgi güvenliği risklerinin zamanında tespit edilmesini ve etkili şekilde yönetilmesini temin ederek operasyonel, finansal ve itibar risklerini azaltmak,
- Bilgi Güvenliği Yönetim Sistemi'nin sürekliliğini ve etkinliğini sağlayarak sistemin zaman içerisinde geliştirilmesini desteklemek.

7. YÜRÜRLÜK

İşbu **Bilgi Güvenliği Politikası**, 26.12.2025 tarihli **Yönetim Kurulu kararı** ile onaylanarak yürürlüğe girmiştir. Politika hükümleri, yürürlüğe girdiği tarihten itibaren Bera Holding A.Ş. ve bağlı ortaklıkları bünyesinde uygulanır.

Bilgi Güvenliği Politikası'nda yapılması gerekli görülen her türlü değişiklik ve güncelleme, Yönetim Kurulu onayını müteakip geçerlilik kazanır. Onaylanan güncel politika; Şirket içi iletişim kanalları aracılığıyla tüm çalışanlara duyurulur, ilgili üçüncü tarafların erişimine sunulur ve Politika hükümlerinin uygulanması izlenir. Politika, mevzuat değişiklikleri, organizasyonel ihtiyaçlar ve risk ortamındaki gelişmeler dikkate alınarak periyodik olarak gözden geçirilir.

8. YÜRÜTME

İşbu Politika hükümleri, **Yönetim Kurulu'nun gözetim ve yetkisi altında** yürütülür. Politika'nın uygulanmasına ilişkin operasyonel sorumluluklar, Yönetim Kurulu tarafından yetkilendirilen **Üst Yönetim** ve ilgili birimler aracılığıyla yerine getirilir. Yönetim Kurulu, Politika'nın etkin şekilde uygulanmasını ve sürdürülebilirliğini teminen gerekli yönlendirmeleri yapar ve gözetim faaliyetlerini yürütür.