ZERAY GAYRİMENKUL YATIRIM ORTAKLIĞI A.Ş.
BİLGİ SİSTEMLERİ YÖNETİMİ POLİTİKASI

1. Amaç ve Kapsam

İşbu Bilgi Sistemleri Yönetimi Politikası'nın ("Politika") amacı; Zeray Gayrimenkul Yatırım Ortaklığı A.Ş.'nin ("Şirket") kurumsal hedefleri ve yasal yükümlülükleri doğrultusunda, sahip olduğu bilgi sistemlerinin ve bilgi varlıklarının gizlilik, bütünlük, erişilebilirlik, doğruluk, süreklilik ve mevzuata tam uyum ilkeleri çerçevesinde yönetilmesine ilişkin temel esasları, idari ve teknik kontrolleri belirlemektir.

Bu Politika; Şirket'in bilgi sistemleri yönetimi süreçlerinin etkin bir şekilde işletilmesi için gerekli olan kurumsal rollerin, sorumlulukların ve görev tanımlarının belirlenmesini, bilgi sistemleri hedeflerinin oluşturulmasını, proaktif risk yönetimini, tesis edilen bilgi güvenliği kontrollerini, dış hizmet ve bulut sağlayıcılarının gözetim mekanizmalarını, erişim ve yetkilendirme standartlarını, log/kayıt yönetimini, siber olay ve ihlal yönetim süreçlerini, iş sürekliliği ve yedekleme esaslarını kapsar.

Politika; Şirket'in tüm iş birimlerini, çalışanlarını, yöneticilerini, bilgi sistemleri üzerinde yetkilendirilen tüm kullanıcıları, Şirket adına veya Şirket nezdinde bilgi sistemlerine erişim sağlayan üçüncü tarafları, dış hizmet sağlayıcılarını, danışmanları ve Şirket'in sahip olduğu, kullandığı, işlediği veya dış hizmet sağlayıcıları altyapısında güvenli şekilde bulundurduğu tüm bilgi varlıklarını kapsar.

Şirket çalışanları ve Şirket bilgi sistemlerine erişim sağlayan tüm üçüncü taraflar, işbu Politika'ya ve bu Politika'nın ayrılmaz bir parçası olan alt prosedür, talimat, duyuru ve kullanım kurallarına istisnasız olarak uymakla yükümlüdür.

2. Dayanak

Zeray Gayrimenkul Yatırım Ortaklığı A.Ş. ("Şirket") Bilgi Sistemleri Yönetimi Politikası; 6102 sayılı Türk Ticaret Kanunu, 6362 sayılı Sermaye Piyasası Kanunu ("SPKn"), Sermaye Piyasası Kurulu ("SPK") tarafından yayımlanan VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği ile II-17.1 sayılı Kurumsal Yönetim Tebliği, 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK"), vergi mevzuatı, ilgili diğer yasal mevzuat ve Şirket Esas Sözleşmesi hükümleri uyarınca hazırlanmıştır.

Söz konusu yasal düzenlemelerde halka açık ortaklıklar ve gayrimenkul yatırım ortaklıkları bakımından öngörülen muafiyet sınırları ve özel hükümler saklı kalmak kaydıyla, Şirket'in tabi olduğu tüm yasal ve kurumsal yükümlülüklerin eksiksiz bir şekilde yerine getirilmesi esastır.

3. Genel İlkeler

Şirket, bilgi sistemleri yönetimini kurumsal yönetişim ilkelerinin asli ve ayrılmaz bir parçası olarak kabul eder. Bilgi sistemlerinin, Şirket faaliyetlerinin güvenli, kesintisiz, mevzuata uygun, şeffaf ve denetlenebilir şekilde yürütülmesini destekleyecek yapıda kurgulanması ve işletilmesi temel felsefedir.

Bu doğrultuda Şirket, aşağıda belirtilen temel ilkeleri rehber edinir:

- Bilgi sistemleri yönetimine ve güvenliğine ilişkin süreçlerin yazılı, ölçülebilir ve güncel dokümantasyonla yürütülmesi,

- Bilgi sistemlerine yönelik risklerin düzenli olarak analiz edilmesi, izlenmesi ve gerekli proaktif önlemlerin zamanında alınması,
- Şirket genelinde bilgi varlıkları envanterinin güncel tutulması ve kritiklik seviyelerinin net olarak tanımlanması,
- Erişim ve yetkilendirme süreçlerinin "görevler ayrılığı" ve "en az yetki" (need-to-know) prensiplerine dayalı olarak yürütülmesi,
- Dış hizmet ve bulut bilişim hizmetlerinin yasal mevzuata uyum çerçevesinde sürekli gözetim altında tutulması,
- Denetim izi (log) kayıtlarının mevzuatın öngördüğü standartlarda, bütünlüğü korunarak ve zaman damgasıyla tutulması,
- Bilgi güvenliği ihlallerinin veya şüphelerinin anında tespiti, kayıt altına alınması, müdahale edilmesi ve raporlanması,
- İş sürekliliği ve yedekleme süreçlerinin olası kesintilere karşı iş süreçlerini koruyacak şekilde kararlılıkla işletilmesi,
- Çalışanların bilgi güvenliği farkındalığının sürekli eğitimlerle dinamik tutulması.

4. Rol ve Sorumluluklar

4.1. Yönetim Kurulu

Yönetim Kurulu, bilgi sistemleri yönetimi ve bilgi güvenliği süreçlerinin Şirket'in faaliyet ölçeği, risk profili ve tabi olduğu mevzuat çerçevesinde yapılandırılmasını, gerekli iç kontrol mekanizmalarının tesis edilmesini en üst düzeyde gözetir. İşbu Politika ve Politika'da yapılacak esaslı değişiklikler Yönetim Kurulu onayına tabidir.

4.2. Üst Yönetim

Üst Yönetim, bu Politika'nın Şirket'in tüm operasyonlarında eksiksiz uygulanmasını gözetir; bilgi sistemleri yönetimine ilişkin politika, prosedür ve süreçlerin oluşturulması, güncellenmesi ve ilgili taraflara duyurulması için gerekli koordinasyonu sağlar. Bilgi güvenliği yatırımları, risk yönetimi, iş sürekliliği, dış hizmet sağlayıcılarının yasal uyum gözetimi ve farkındalık eğitimleri için ihtiyaç duyulan kaynakların tahsis edilmesini güvence altına alır.

Bu Politika kapsamında Üst Yönetim, Yönetim Kurulu tarafından belirlenen kişi veya kurulu; böyle bir belirleme yapılmamışsa Şirket'in en üst icra yetkilisini (Genel Müdür/CEO) ifade eder.

4.3. Bilgi Güvenliği ve Uyum Sorumlusu

Şirket bünyesinde bilgi sistemleri güvenliği, regülasyonlara uyum ve denetim süreçlerinin takibinden sorumlu bir kişi veya birim görevlendirilir. Bu sorumlu, icrai ve operasyonel bilişim süreçlerinden bağımsız olarak süreçlerin uygunluğunu denetler; tespit edilen riskleri, uyum ihtiyaçlarını ve geliştirme alanlarını doğrudan Üst Yönetim'e raporlar.

Bilgi Güvenliği ve Uyum Sorumlusu'nun temel görevleri şunlardır:

- Bilgi sistemleri üst politikası ile bağlı alt prosedürlerin mevzuata uyumlu şekilde hazırlanmasını ve güncelliğini koordine etmek,
- Bilgi sistemleri risk analizi çalışmalarının takibini yürütmek ve raporlamak,
- Erişim yetkilendirmeleri ile kullanıcı hesap yönetimi süreçlerinin yazılı kurallara uygunluğunu periyodik olarak gözetmek,
- Dış hizmet ve bulut sağlayıcılarının bilgi güvenliği, veri koruma (KVKK) ve sözleşmesel taahhütlerini yasal yönden değerlendirmek,
- Bilgi güvenliği ihlalleri veya olaylarında; kayıt, analiz, kök neden analizi ve mevzuat uyarınca yapılması gereken kurumsal bildirim süreçlerini koordine etmek,
- Şirket personeline yönelik bilgi güvenliği ve siber farkındalık çalışmalarını planlamak ve yürütülmesini sağlamak,
- Sermaye piyasası mevzuatındaki ve bilişim hukukundaki değişiklikleri takip ederek sistemlerin sürekli güncel kalmasını sağlamak.

4.4. Bilgi Teknolojileri Birimi

Bilgi Teknolojileri Birimi; Şirket'in sahip olduğu merkezi bilgi sistemleri altyapısının kesintisiz işletilmesinden, donanım ve yazılım varlıklarının teknik yönetiminden, erişim ve yetki tanımlamalarının sistem üzerinde güvenli şekilde uygulanmasından, yedekleme ve geri dönüş işlemlerinin yürütülmesinden, firewall (güvenlik duvarı) ve diğer siber güvenlik bileşenlerinin konfigürasyonundan, teknik logların tutulmasından ve dış hizmet sağlayıcıları ile teknik koordinasyonun yürütülmesinden sorumludur.

Bilgi Teknolojileri Birimi, tüm operasyonlarını işbu Politika ve bağlı teknik talimatlar doğrultusunda gerçekleştirir.

4.5. Çalışanlar

Şirket çalışanları, kendilerine tahsis edilen tüm bilişim kaynaklarını, bilgisayarları, ağ altyapısını ve bilgi varlıklarını yalnızca görev tanımları, yetkileri ve kurumsal amaçlar kapsamında kullanmakla yükümlüdür. Çalışanlar;

- Kullanıcı adı, parola, MFA (Çok Faktörlü Kimlik Doğrulama) kodları ve benzeri kişisel kimlik doğrulama bilgilerini mutlak surette gizli tutar, üçüncü şahıslarla paylaşmaz,
- Yetkisi bulunmayan veya iş ihtiyacı olmayan sistemlere, veri tabanlarına, klasör ve dosyalara erişim sağlama girişiminde bulunmaz,
- Şirket bilgi sistemlerini hukuka, sermaye piyasası düzenlemelerine, iş etiğine ve kurumsal disiplin kurallarına aykırı amaçlarla kullanmaz,
- Herhangi bir bilgi güvenliği zafiyeti, ihlali veya siber olay şüphesi (örn: şüpheli e-posta, zararlı yazılım uyarısı vb.) fark ettiğinde durumu derhal Bilgi Teknolojileri Birimi'ne ve Bilgi Güvenliği Sorumlusu'na bildirir,
- Şirket tarafından ilan edilen tüm bilişim kurallarına ve güvenlik talimatlarına tam uyum sağlar.

4.6. Üçüncü Taraflar ve Dış Hizmet Sağlayıcılar

Şirket adına veya Şirket sistemlerine entegre şekilde bilgi sistemlerine erişim sağlayan üçüncü taraflar, tedarikçiler ve dış hizmet sağlayıcıları; kendilerine tebliğ edilen bilgi güvenliği kurallarına, imzalanan gizlilik sözleşmelerine (NDA) ve ilgili yasal mevzuata tam olarak uymak zorundadır. Üçüncü taraflara sağlanan erişim yetkileri, yalnızca aldıkları hizmetin kapsamı ve süresi ile sınırlı tutulur; "en az yetki" prensibi teknik olarak uygulanır.

5. Bilgi Sistemleri Risk Yönetimi

Bilgi sistemlerine yönelik risklerin yönetimi, Şirket'in Kurumsal Risk Yönetimi altyapısının ayrılmaz bir parçası olarak aktif şekilde işletilir.

Şirket; bilgi sistemleri varlıklarına, altyapısına ve iş süreçlerine yönelik tehdit ile zafiyetleri belirlemek, risklerin olası etkilerini ve gerçekleşme olasılıklarını ölçmek, bunları izlemek ve kabul edilebilir seviyelere indirmek üzere yapılandırılmış bir risk yönetimi süreci yürütür. Risk değerlendirme çalışmalarında özellikle aşağıdaki kritik odak alanları dikkate alınır:

- Bilgi sistemlerine bağımlı olarak yürütülen operasyonel iş süreçleri,
- Dış hizmet, yazılım ve bulut bilişim teknolojilerinin kullanımı,
- Kullanıcı erişimleri, ayrıcalıklı hesaplar ve yetki dağılımları,
- Kişisel verilerin (KVKK), ticari sırların ve kritik finansal verilerin güvenliği,
- Log/kayıt yönetimi ve izlenebilirlik,
- Bilgi güvenliği ihlalleri, siber saldırılar ve oltalama (phishing) riskleri,
- İş sürekliliği gereksinimleri, felaket kurtarma ve yedekleme kapasiteleri,
- Sermaye piyasası ve GYO mevzuatından kaynaklanan uyum yükümlülükleri.

Bilgi sistemlerine ilişkin risk analizi ve değerlendirme çalışmaları yılda en az bir kez periyodik olarak gerçekleştirilir. Şirket organizasyonunda, kritik iş süreçlerinde, kullanılan temel uygulamalarda veya dış hizmet altyapısında majör bir değişiklik meydana gelmesi durumunda risk analizi döngü süresi beklenmeksizin yenilenir. Risk analizleri sonucunda belirlenen iyileştirici faaliyetler, aksiyon planları, sorumluları ve hedef tarihleriyle birlikte kayıt altına alınarak Üst Yönetim'in onayına ve takibine sunulur.

6. Bilgi Varlıkları Yönetimi

Şirket bünyesinde üretilen, işlenen veya saklanan tüm değerli veriler ile bunları barındıran donanım, yazılım ve ağ bileşenleri "Bilgi Varlığı" olarak tanımlanır ve kurumsal bir envanter yapısında takip edilir.

Bilgi varlığı envanterinde asgari olarak; varlığın adı ve teknik tanımı, kurumsal varlık sahibi (owner), kullanıcıları veya ilgili iş birimi, bulunduğu fiziksel/mantıksal ortam, gizlilik ve kritiklik sınıfı, yedekleme stratejisi ve varsa ilişkili dış hizmet sağlayıcı bilgileri yer alır.

Bilgi varlıkları; gizlilik, bütünlük ve erişilebilirlik (G-B-E) kriterleri, kişisel veri içerme durumları, finansal raporlama ve kamuyu aydınlatma süreçlerine etkileri, operasyonel kritiklikleri ve yasal önemleri doğrultusunda objektif bir matrisle sınıflandırılır.

Kullanımdan kaldırılan, ömrünü tamamlayan donanımlar, yazılımlar, kullanıcı hesapları, uygulamalar veya veri depolama ortamları (sabit disk, taşınabilir medya vb.) üzerinde bulunan Şirket verileri, geri döndürülemeyecek şekilde güvenli silme (wiping) yöntemleri veya fiziksel imha işlemleriyle yok edilir ve bu süreçler tutanak altına alınarak arşivlenir.

7. Erişim ve Yetkilendirme

Şirket bilgi sistemlerine ve kurumsal ağa erişimler; iş ihtiyacı (need-to-know), görevler ayrılığı (segregation of duties) ve en az yetki (least privilege) prensipleri çerçevesinde katı kurallarla kontrol altında tutulur.

Kullanıcı hesabı açılması, yetki tanımlanması, yetki değişiklikleri, yetki iptali, rol değişiklikleri, işten ayrılma süreçleri ve ayrıcalıklı hesapların (admin/root) yönetimi yazılı prosedürlere göre yürütülür. Erişim ve yetkilendirme süreçlerinde aşağıdaki temel kurallar esastır:

- Her kullanıcıya, sistem üzerindeki işlemlerinin izlenebilirliğini ve hesap verilebilirliğini sağlamak amacıyla benzersiz (tekil) bir kurumsal kullanıcı hesabı tanımlanır.
- Ortak veya anonim kullanıcı hesaplarının kullanımı kesinlikle sınırlandırılır ve yalnızca teknik zorunluluk hallerinde, ek denetim izleri oluşturularak izin verilir.
- Yetki tanımlamaları, personelin güncel görev tanımı ve iş gereksinimleri ile tam uyumlu olacak şekilde asgari düzeyde tutulur.
- Görevi değişen veya Şirket ile ilişiği kesilen (işten ayrılma, sözleşme feshi vb.) personelin erişim yetkileri ve kullanıcı hesapları, İnsan Kaynakları bildirimi doğrultusunda Bilgi Teknolojileri Birimi tarafından gecikmeksizin ve mümkün olan en kısa sürede askıya alınır veya kapatılır.
- Sistemlerin yönetici yetkilerine sahip ayrıcalıklı hesapları (domain admin, global admin vb.) sadece sınırlı sayıda teknik uzmana yetkileri dahilinde verilir ve bu hesapların faaliyetleri yakından izlenir.
- Şirket ağı dışından kurumsal sistemlere yapılacak tüm uzaktan erişimlerde güvenli, şifrelenmiş bağlantı yöntemleri (VPN vb.) ve çok faktörlü kimlik doğrulama (MFA) mekanizmaları zorunlu olarak uygulanır.
- Kullanıcı erişim yetkileri ve rol dağılımları, Bilgi Teknolojileri Birimi ve İş Birimi yöneticileri tarafından belirli aralıklarla düzenli olarak gözden geçirilir, güncellenir ve kayıt altına alınır.

8. Parola ve Kimlik Doğrulama Kuralları

Kullanıcılar, kendilerine tahsis edilen kullanıcı adı, güçlü kurumsal parola, MFA doğrulama kodları ve dijital sertifika gibi kimlik doğrulama bileşenlerinin güvenliğinden ve gizliliğinden şahsen sorumludur.

Kurumsal parolalar; kolay tahmin edilebilir, ardışık veya kişisel bilgiler içeren yapıda olamaz. Kullanıcılar parolalarını hiçbir koşulda üçüncü kişilerle (iş arkadaşları ve BT personeli dahil) paylaşamaz, yazılı olarak açık ortamlarda bulunduramaz ve tarayıcılara güvensiz şekilde kaydedemez.

Bilgi Teknolojileri Birimi; kurumsal sistemlerde parola uzunluğu, karakter karmaşıklığı (büyük/küçük harf, rakam, özel karakter), maksimum parola ömrü (değiştirme periyodu), hatalı giriş denemelerinde hesap kilitleme süresi ve aktif oturum zaman aşımı (session timeout) gibi teknik güvenlik kurallarını merkezi grup politikaları (Group Policy/GPO) üzerinden zorunlu kılar ve sürekli olarak yürütür.

9. Dış Hizmet, Bulut ve Tedarikçi Yönetimi

Şirket; operasyonel verimliliği, teknolojik çevikliği ve hizmet kalitesini artırmak amacıyla bilgi sistemleri süreçlerinde nitelikli dış hizmet ve bulut bilişim çözümlerinden yararlanır. Bu kapsamda Şirket altyapısında; kurumsal e-posta ve bulut üretkenlik süreçlerinde Microsoft Office 365, kurumsal kaynak planlama, müşteri ilişkileri ve finans/muhasebe süreçlerinde IFS ERP, gayrimenkul ve proje yönetiminde Yapıtaşı ve personel devam kontrol sistemlerinde Meyer PDKS gibi endüstriyel çözümler aktif ve güvenli bir şekilde kullanılır.

Dış hizmet ve bulut bilişim hizmetlerinin alımı, yönetimi ve denetiminde aşağıdaki kurumsal esaslar uygulanır:

- Herhangi bir dış hizmet veya bulut çözümü devreye alınmadan önce, hizmetin niteliği, kritiklik seviyesi, iş sürekliliğine etkisi, siber güvenlik riskleri ve sağlayıcının teknik/yasal yeterliliği (özellikle veri barındırma lokasyonlarının KVKK uyumu) detaylı olarak analiz edilir.
- Dış hizmet sağlayıcılar ile akdedilen sözleşmelerde; hizmetin net kapsamı, Hizmet Seviyesi Taahhütleri (SLA), bilgi güvenliği ve gizlilik yükümlülükleri, erişim sınırları, veri yedekleme ve bütünlük garantileri, siber olay ihlal bildirim süreleri ve gizlilik sözleşmeleri (NDA) yasal olarak güvence altına alınır.
- Hizmet sağlayıcı personeline Şirket sistemlerine veya verilerine yönelik olarak verilecek erişim izinleri, sadece ilgili işin ifası için gerekli olan süre ve kapsamla sınırlandırılır ve sürekli izlenir.
- Hizmet ilişkisi sonlandırıldığında; Şirket'e ait tüm verilerin, yedeklerin ve kaynak kodların güvenli bir şekilde Şirket'e iade edilmesi, aktarılması ve sağlayıcı sistemlerinden geri döndürülemeyecek şekilde silinmesi/imha edilmesi yükümlülüğü sözleşmelerle yasal olarak karara bağlanır.
- Kullanılan kritik dış hizmet ve bulut sağlayıcılarının güvenlik ve uyum performansları, bağımsız denetim raporları (SOC 2, ISO 27001 vb.) ve kurumsal izleme mekanizmaları üzerinden periyodik olarak değerlendirilir.

Dışarıdan hizmet veya bulut hizmeti alınması, Şirket'in sermaye piyasası mevzuatından ve diğer yasal düzenlemelerden kaynaklanan nihai sorumluluklarını ortadan kaldırmaz. Stratejik karar alma, gözetim ve nihai yönetim sorumluluğu her halükarda Şirket'e aittir.

10. Log / Kayıt Yönetimi ve İzleme

Şirket, bilgi sistemlerinin güvenliğini sağlamak, olağan dışı aktiviteleri tespit etmek ve yasal uyum gereksinimlerini karşılamak amacıyla gelişmiş bir denetim izi (log) kayıt ve izleme mimarisi işletir.

Kritik bilgi sistemleri, kullanıcı oturum hareketleri, yetki ve rol değişiklikleri, hassas veri tabanı erişimleri, sistem yöneticisi (admin) işlemleri, güvenlik duvarı kurallarındaki değişiklikler, yetkisiz erişim denemeleri ve sistem konfigürasyonlarında değişikliğe sebep olan tüm operasyonlar anlık olarak kayıt altına alınır.

Oluşturulan denetim izlerinde; işlemin türü ve niteliği, işlemi gerçekleştiren kullanıcı veya sistem hesabı, işlemin gerçekleştiği kesin zaman (zaman damgası), işlemin başarı/başarısızlık sonucu, erişilen sistem/uygulama/klasör bileşenleri ve işlem yapılan kaynak IP adresleri eksiksiz olarak tutulur.

Şirket'in ağ trafiği, internet erişimleri ve sınır güvenliği olayları Fortinet Firewall altyapısı ve merkezi log yönetim mekanizmaları üzerinden kesintisiz olarak izlenir, analiz edilir ve anomaliler tespit edilir. Log yönetim süreçlerinin teknik detayları, kayıtların bütünlüğünün (hashing/kriptografik yöntemlerle) korunması, saklama süreleri, yetkisiz değiştirmeye karşı korunması ve analiz esasları ilgili alt prosedürlerle düzenlenir.

Kullanıcılar, Şirket bilgi sistemleri, kurumsal ağ ve internet altyapısı üzerinde gerçekleştirdikleri tüm işlemlerin mevzuata, iş sözleşmelerine ve kurumsal politikalara uygunluğun denetlenmesi amacıyla yasal sınırlar dahilinde kayıt altına alınabileceği ve izlenebileceği konusunda bilgilendirilir.

11. Bilgi Güvenliği İhlalleri ve Olay Yönetimi

Şirket, siber güvenlik tehditlerine, veri sızıntılarına, güvenlik açıklarına ve şüpheli faaliyetlere karşı hızlı, etkin ve koordineli bir şekilde yanıt verebilmek adına kurumsal bir Siber Olay Müdahale ve İhlal Yönetimi süreci işletir.

Çalışanlar, iş ortakları ve üçüncü taraflar; herhangi bir bilgi güvenliği ihlali, kişisel veri sızıntısı şüphesi, yetkisiz erişim tespiti, oltalama e-postası, zararlı yazılım bulaşması, kurumsal cihaz kaybı (laptop, şirket telefonu vb.) veya yanlış alıcıya hassas veri gönderimi gibi bir durumla karşılaştıklarında, durumu gecikmeksizin Bilgi Teknolojileri Birimi'ne ve Bilgi Güvenliği Sorumlusu'na bildirmekle yükümlüdür.

Tüm bilgi güvenliği olayları merkezi bir takip sisteminde kayıt altına alınır. Olayın analizi, etkilenen sistemler, veri kategorileri, olayın kök nedeni, alınan acil durdurma ve giderme aksiyonları ile geleceğe yönelik önleyici faaliyetler detaylı olarak raporlanır.

Meydana gelen olayın kişisel verileri (KVKK) etkileme ihtimali bulunması durumunda, yasal süreler (72 saat) dahilinde Kişisel Verileri Koruma Kurulu'na ve etkilenen ilgili kişilere bildirim yapılması süreçleri Hukuk Müdürlüğü koordinasyonunda yürütülür. SPK mevzuatı uyarınca kamuyu aydınlatma veya kurumsal bildirim yükümlülüğü doğuran siber olaylar ise ilgili yasal süreler içinde Sermaye Piyasası Kurulu'na ve ilgili mercilere raporlanır.

12. Bilgi Sistemleri Sürekliliği ve Yedekleme

Şirket, olağanüstü durumlar, siber saldırılar, donanım arızaları veya fiziksel felaketler karşısında kritik iş süreçlerinin kesintisiz devam etmesini güvence altına almak amacıyla kararlı bir Bilgi Sistemleri İş Sürekliliği ve Felaket Kurtarma yaklaşımı benimser.

Yedekleme stratejileri; bilgi varlıklarının kritiklik dereceleri, Hedeflenen Kurtarma Noktası (RPO) ve Hedeflenen Kurtarma Süresi (RTO) parametreleri, kullanılan kurumsal sistemlerin

(IFS, Yapıtaşı vb.) teknik gereksinimleri ve bulut sağlayıcılarının (Microsoft Office 365) sunduğu yüksek erişilebilirlik imkânları gözetilerek yapılandırılır. Yedekleme süreçlerinde aşağıdaki temel kurallar titizlikle uygulanır:

- Kritik sistemler, veri tabanları ve kullanıcı verileri için belirlenmiş kurumsal frekanslarda (günlük, haftalık, aylık) otomatik yedekleme senaryoları çalıştırılır.
- Yedekleme operasyonlarının başarı durumları her gün Bilgi Teknolojileri Birimi tarafından kontrol edilir ve loglanır.
- Alınan yedeklerin güvenliği, şifrelenmiş ortamlarda tutulması ve yetkisiz erişimlere karşı korunması teknik olarak sağlanır. Olası fidye yazılımı (ransomware) saldırılarına karşı verilerin değiştirilemez (immutable/offline) yedek kopyaları oluşturulur.
- Alınan yedeklerin doğruluğunu ve sistemlerin geri yüklenebilirliğini doğrulamak amacıyla, belirlenen periyotlarda yedekten geri dönüş (restore) testleri uygulanır ve test sonuçları raporlanır.
- Dış hizmet ve bulut sağlayıcılarının yedekleme, veri replikasyonu ve coğrafi yedlilik altyapıları sözleşmesel taahhütler çerçevesinde periyodik olarak kontrol edilir.

Bilgi sistemleri süreklilik planları ve yedekleme politikaları, yılda en az bir kez veya altyapıda majör bir mimari değişiklik yapılması durumunda gözden geçirilerek güncellenir.

13. Veri Güvenliği ve Gizlilik

Şirket; bilgi sistemleri kanalıyla üretilen, işlenen, aktarılan ve saklanan tüm kurumsal verilerin, finansal kayıtların, yatırımcı bilgilerinin, proje detaylarının, ticari sırların ve kişisel verilerin yetkisiz erişime, sızıntıya, kayba, tahrifata veya kötüye kullanıma karşı korunması amacıyla gerekli tüm idari ve teknik tedbirleri en üst düzeyde uygular.

Kişisel verilerin işlenmesi ve güvenliği süreçlerinde, 6698 sayılı Kanun ve Kişisel Verileri Koruma Kurumu düzenlemeleri tam bir uyumla işletilir. Veriler, taşıdıkları risk ve gizlilik derecesine göre şifrelenmiş (at-rest ve in-transit encryption) veri depolama alanlarında saklanır.

Şirket'e ait hiçbir gizli belge, rapor, stratejik yatırım kararı, proje çizimi veya kişisel veri; yetkilendirme ve meşru kurumsal amaçlar dışında üçüncü şahıslarla paylaşılamaz, kopyalanamaz ve şirket dışına çıkarılamaz.

14. Elektronik Posta ve İnternet Kullanımı

Şirket tarafından çalışanlara tahsis edilen elektronik posta hesapları (...@zeraygyo.com.tr) ve kurumsal internet hatları, öncelikli olarak Şirket faaliyetlerinin ve iş süreçlerinin etkin bir şekilde yürütülmesi amacıyla kullanılır.

Çalışanlar, kurumsal iletişim kuralları çerçevesinde; e-posta hesaplarını iş etiğine uygun kullanır, oltalama (phishing) saldırılarına karşı şüpheli e-posta eklentilerini ve bağlantılarını açmamakla, lisanssız veya iş dışı yazılım/dosya indirmemekle yükümlüdür. Şirket ağ kaynaklarının; yasa dışı, genel ahlaka aykırı, fikri mülkiyet haklarını ihlal eden veya Şirket'in kurumsal itibarını zedeleyebilecek nitelikteki internet sitelerine erişim veya içerik paylaşımı amacıyla kullanılması kesinlikle yasaktır ve teknik filtreleme araçlarıyla (web filtering) engellenir.

15. Zararlı Yazılımlardan Korunma ve Uç Nokta Güvenliği

Şirket, bilgi sistemleri altyapısını ve uç noktaları (sunucular, kullanıcı bilgisayarları, mobil cihazlar) virüs, truva atı, fidye yazılımı gibi zararlı kodlara ve gelişmiş siber tehditlere karşı korumak amacıyla merkezi güvenlik mimarileri uygular.

Tüm kurumsal bilgisayarlarda ve sunucularda, merkezi olarak yönetilen ve güncellenen anti-virüs / uç nokta koruma (EDR) yazılımları aktif olarak çalışır. Kullanıcıların bu yazılımları devre dışı bırakması, ayarlarını değiştirmesi veya sistemlere BT biriminin onayı dışında harici depolama birimleri (güvensiz USB bellek vb.) bağlaması teknik politikalarla sınırlandırılır. İşletim sistemi ve kritik uygulama güvenlik yamaları (patch management) merkezi sistemler üzerinden düzenli olarak kontrol edilir ve yüklenir.

16. Yazılım Kullanımı ve Lisans Yönetimi

Şirket bilgi sistemlerinde ve kullanıcı bilgisayarlarında yalnızca lisanslı, telif hakları yasal olarak satın alınmış, Şirket standartlarına uygun ve iş ihtiyacını karşılayan onaylı yazılımlar kullanılabilir.

Çalışanların, Bilgi Teknolojileri Birimi'nin bilgisi ve teknik onayı olmaksızın bilgisayarlarına internetten açık kaynak, ücretsiz, deneme sürümü, lisanssız veya kaynağı doğrulanmamış yazılımlar indirmesi, kurması ve çalıştırması kesinlikle yasaktır. Şirket'e ait yazılımlar ve lisans anahtarları kopyalanamaz, şirket dışına çıkarılamaz. Yazılım ve lisans envanterlerinin takibi, optimizasyonu ve yasal uyum denetimleri Bilgi Teknolojileri Birimi tarafından düzenli olarak gerçekleştirilir.

17. Eğitim ve Farkındalık

Şirket, bilgi güvenliği kültürünü kurumsal düzeyde yaygınlaştırmak ve insan faktöründen kaynaklanabilecek siber riskleri minimize etmek amacıyla sürekli bir eğitim ve farkındalık programı yürütür.

Tüm Şirket çalışanlarına; güvenli parola yönetimi, e-posta güvenliği, sosyal mühendislik ve kimlik avı (oltalama) saldırılarına karşı korunma yöntemleri, veri gizliliği (KVKK), temiz masa-temiz ekran ilkesi ve siber olay bildirim kanalları hakkında periyodik olarak farkındalık eğitimleri verilir, bilgilendirme duyuruları yayımlanır. Şirket bünyesinde işe yeni başlayan tüm personelin oryantasyon sürecine bilgi güvenliği kuralları eğitimi zorunlu olarak dahil edilir. Eğitim faaliyetleri ve katılım durumları kayıt altına alınarak izlenir.

18. Politikanın Duyurulması

İşbu Politika ve Politika kapsamında yürürlüğe konulan prosedür, talimat ve rehberler; kapsamına ve hedef kitlesine göre tüm Şirket çalışanlarına, yöneticilerine, ilgili üçüncü taraflara ve dış hizmet sağlayıcılarına kurumsal iletişim kanalları üzerinden tebliğ edilir ve duyurulur. Politika'nın, kurumsal şeffaflık ve yatırımcı ilişkileri çerçevesinde Şirket'in resmi internet sitesinde yayımlanması mümkündür.

19. İzleme ve Denetleme Hakları

Şirket; bilgi varlıklarının güvenliğini sağlamak, yasal mevzuata (SPK, KVKK, 5651 sayılı Kanun vb.) tam uyumu doğrulamak, iş sürekliliğini korumak ve kurumsal kuralların ihlal

edilmesini önlemek amacıyla, bilgi sistemlerinin ve kurumsal ağ kaynaklarının kullanımına ilişkin her türlü log, erişim ve trafik kaydını yasal sınırlar çerçevesinde tutma, izleme, otomatik araçlarla analiz etme ve gerektiğinde inceleme hakkına sahiptir.

Bu izleme faaliyetleri neticesinde elde edilen kayıtlar, sadece yetkilendirilmiş personel tarafından, münhasıran meşru güvenlik ve uyum amaçlarıyla işlenir; adli ve idari makamlar ile ancak yasal mevzuatın zorunlu kıldığı hallerde ve usulüne uygun olarak paylaşılır.

20. Alt Politika, Prosedür ve Talimatlar

İşbu üst düzey Bilgi Sistemleri Yönetimi Politikası'nın operasyonel altyapısını oluşturmak üzere; yasal mevzuat, uluslararası standartlar ve Şirketimiz siber risk profili ile uyumlu aşağıdaki alt dokümantasyon yapısı (prosedür, talimat ve rehberler) tasarlanarak Yönetim Kurulu kararı tarihinden itibaren en geç 6 (altı) ay içerisinde hazırlanır ve Üst Yönetim onayı ile yürürlüğe konulur:

- Bilgi Varlıklarının Sınıflandırılması ve Envanter Yönetimi Prosedürü,
- Kullanıcı Hesapları, Erişim ve Yetkilendirme Yönetimi Prosedürü,
- Kurumsal Parola Standartları ve Kimlik Doğrulama Talimatı,
- Dış Hizmet, Bulut Sağlayıcıları ve Tedarikçi Güvenliği Prosedürü,
- Log (Denetim İzi) Yönetimi, Saklama ve İzleme Prosedürü,
- Siber Olay Müdahale ve Bilgi Güvenliği İhlal Yönetimi Prosedürü,
- Sistem Yedekleme, Güvenlik ve Geri Dönüş Testleri Prosedürü,
- Kurumsal E-Posta, İnternet ve İletişim Kaynakları Güvenli Kullanım Talimatı,
- Yazılım Varlıkları ve Lisans Yönetimi Talimatı,
- Bilgi Güvenliği Farkındalık Eğitimi ve Sosyal Mühendislik Test Prosedürü.

Teknolojik yenilikler, risk analiz sonuçları veya mevzuat güncellemeleri doğrultusunda Üst Yönetim onayı ile yeni alt prosedürler ve rehberler devreye alınabilir. Şirket, sürekli gelişim prensibi doğrultusunda yürürlüğe giren bu dokümanları güncel tutar.

21. Sürekli Gelişim ve Uyum Yönetimi

Şirket'in kurumsal bilgi sistemleri altyapısı, aktif olarak kullanılan endüstriyel yazılımlar (IFS, Yapıtaşı, Microsoft Office 365 vb.), sınır güvenliği bileşenleri (Fortinet) ve idari kontroller, işbu Politikada yer alan yüksek standartları halihazırda karşılayacak seviyede işletilir.

Şirket, gelişen siber tehdit ortamına ve sermaye piyasası düzenlemelerindeki güncellenen standartlara tam uyumu sürekli kılmak amacıyla, bilgi sistemleri kontrollerini düzenli iç değerlendirmelere ve teknik danışmanlık incelemelerine tabi tutar. Bu doğrultuda belirlenen proaktif teknolojik optimizasyonlar, sistem güncellemeleri ve süreç geliştirme faaliyetleri, dinamik bir plan dahilinde Üst Yönetim'in gözetiminde kesintisiz olarak yürütülür.

22. Aykırılık ve Yaptırımlar

İşbu Politika hükümlerine, bağlı alt prosedürlere, güvenlik talimatlarına ve ilan edilen kurallara aykırı hareket ettiği, kasıtlı veya ağır ihmal neticesinde bilgi güvenliği ihlaline, veri sızıntısına veya Şirket'in yasal riske girmesine neden olduğu tespit edilen personel hakkında, ihlalin niteliği ve boyutuna göre Zeray Gayrimenkul Yatırım Ortaklığı A.Ş. Disiplin Yönetmeliği ve ilgili iş mevzuatı hükümleri uygulanır. Aykırılığın niteliğine göre iş sözleşmesinin haklı nedenle feshi dahil gerekli disiplin cezaları verilebilir. Şirket'in maddi veya itibari zarara uğraması ya da yasal regülasyonlar karşısında cezai müeyyideyle karşılaşması durumlarında, sorumlulara yönelik adli, idari ve cezai yollara başvurulması ve rücu haklarının işletilmesi süreci saklıdır.

23. Gözden Geçirme ve Yürürlük

İşbu Politika, Zeray Gayrimenkul Yatırım Ortaklığı A.Ş. Yönetim Kurulu'nun 30/06/2026 tarihli ve 2026/17 sayılı kararı ile onaylanarak yürürlüğe girmiştir.

Politika dokümanı; yasal mevzuattaki değişiklikler, organizasyonel yapılanmadaki dönüşümler, yeni iş süreçleri, teknolojik altyapı modifikasyonları veya siber risk profilindeki değişimler göz önünde bulundurularak yılda en az bir kez periyodik olarak gözden geçirilir. Gerekli görülen güncellemeler ve revizyonlar Yönetim Kurulu onayına sunularak yürürlüğe konulur.