1. AMAÇ VE KAPSAM

İşbu politika ve prosedürler, **Sinpaş Gayrimenkul Yatırım Ortaklığı A.Ş.'**nin (**Şirket**) operasyonlarını istikrarlı, rekabetçi, gelişen ve güvenli bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejilerinin iş hedefleri ile uyumlu olmasını ve bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin olarak bilginin gizliliğini, bütünlüğünü ve gerektiğinde erişilebilir olmasını sağlamak amacıyla hazırlanmıştır.

İşbu doküman bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetimini kapsar.

İşbu prosedür, Şirket yönetim kurulu kararı ile yürürlüğe girer ve ancak Şirket yönetim kurulu kararı ile değiştirilebilir.

Sinpaş Gayrimenkul Yatırım Ortaklığı A.Ş., faaliyet gösterdiği sermaye piyasası ve gayrimenkul yatırım ortaklığı sektörü gereği, başta Sermaye Piyasası Kurulu (SPK) olmak üzere ilgili tüm düzenleyici ve denetleyici kurumlar tarafından yayımlanan mevzuata tam uyum sağlamayı temel bir ilke olarak benimsemektedir. Bu kapsamda, şirketin bilgi güvenliği yönetimi ve bilgi sistemlerine ilişkin süreçleri, sermaye piyasası kurumları için bağlayıcı nitelikte olan ikincil düzenlemeler çerçevesinde yapılandırılmaktadır.

Bu düzenlemelerin başında **Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği (VII-128.10)** gelmektedir. Anılan tebliğ, sermaye piyasası kurum ve ortaklıklarının bilgi sistemlerinin yönetimine ilişkin organizasyon yapısını, iç kontrol ve risk yönetimi mekanizmalarını, bilgi güvenliği politikalarını, erişim ve yetkilendirme süreçlerini, iş sürekliliği ve siber olaylara müdahale esaslarını düzenlemektedir. Sinpaş GYO A.Ş., bilgi sistemlerinin güvenli, sürdürülebilir ve mevzuata uygun şekilde yönetilmesini teminen bu tebliğ hükümlerini esas almakta ve bilgi güvenliği politikalarını bu çerçevede oluşturmaktadır.

Bununla birlikte, **Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2)** uyarınca, sermaye piyasası kurumlarının bilgi sistemleri belirli periyotlarla bağımsız denetime tabi tutulmaktadır. Bu tebliğ, bilgi sistemleri denetiminin kapsamını, denetçi niteliklerini, denetim raporlarının içeriğini ve SPK'ya sunulmasına ilişkin usul ve esasları düzenlemektedir. Sinpaş GYO A.Ş., bilgi sistemlerinin etkinliği, güvenliği ve mevzuata uygunluğunun teyidi amacıyla bu tebliğ kapsamında gerçekleştirilen bağımsız denetim süreçlerine uyum sağlamaktadır. Ayrıca, **Bilgi Sistemleri Bağımsız Denetim Tebliği (III-62.2)'nde Değişiklik Yapılmasına Dair Tebliğ (III-62.2.b)** ile bilgi sistemleri denetim süreçlerine ilişkin bazı usul ve esaslar güncellenmiş, denetim kapsamı ve raporlama yükümlülükleri yeniden düzenlenmiştir. Bu değişiklikler de Sinpaş GYO A.Ş.'nin bilgi güvenliği ve bilgi sistemleri yönetimi süreçlerinde dikkate alınmakta ve uygulamalara yansıtılmaktadır.

Tüm bu ikincil düzenlemelerin dayanağını oluşturan **6362 sayılı Sermaye Piyasası Kanunu** ise sermaye piyasasında faaliyet gösteren ortaklıkların kurumsal yönetim, iç kontrol, risk yönetimi ve bilgi sistemleri dahil olmak üzere genel yükümlülüklerini belirlemektedir. Sinpaş GYO A.Ş., bilgi güvenliği politikalarını ve uygulamalarını söz konusu kanun ve ilgili SPK tebliğleriyle uyumlu olacak şekilde tesis etmekte ve sürekli olarak güncellemektedir.

2. BİLGİ SİSTEMLERİ EDİNİMİ, GELİŞTİRİLMESİ VE BAKIMI

Temin edilecek bilgi sistemleri yapısının Şirket'in ölçeği, faaliyetleri ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması zorunludur. Yatırım yapılan teknolojilerde üretici bağımsız ve yaygın ürünler tercih edilmelidir. Bilgi sistemleri ihtiyaçları tam, sorunsuz karşılayacak ürünler tercih edilmelidir. Tüm bilgi sistemleri ihtiyaçları, kapasite planlaması yapılarak tespit edilmelidir. Gerekli ihtiyaçlar ivedilikle yönetime sunulmalıdır. Şirket sistemlerinin tamamı (donanım, uygulama yazılımları, paket yazılımlar, işletim sistemleri) periyodik bakım güvencesine alınmalıdır. Bakım yapıldıktan sonra tüm sistem dokümantasyonu güncellenmelidir. Sistem bakımlarının ilgili politika ve standartlar tarafından belirlenmiş kurallara aykırı bir sonuç vermediğinden ve güvenlik açıklarına yol açmadığından emin olmak için periyodik uygunluk ve güvenlik testleri yapılmalıdır.

Bilgi sistemlerinde yapılacak önemli güncellemelerin veya değişikliklerin iş süreçlerini aksatmaması ve bilgi güvenliği riski oluşturmaması için güncelleme veya değişikliklere ilişkin planlama, test ve uygulama adımları detaylı olarak ele alınır. Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılmasını, veri üzerindeki işlemlerin doğru sonuçları üretmesini sağlayacak, veri ve işlem kaybını, verinin yetkisiz değiştirilmesini ve kötüye kullanımını önleyecek uygun kontroller tesis edilir.

Uygulama güvenliği ve erişilebilirlik gereksinimleri belirlenirken risk öncelikleri göz önünde bulundurulur. Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterleri belirlenir, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimleri testlerine tabi tutulur, test verileri özenle seçilerek korunur ve kontrol edilir. Geliştirme, test ve gerçek ortamdaki işlemler ile bu işlemlerin gerçekleştiği ortamlar, yetkisiz erişim ve değişim riskine karşı birbirinden ayrılır.

Gerekli hallerde değiştirilmiş veya yeni geliştirilmiş sistem, gerçek ortamda kullanıma alınmadan önce, belirli bir olgunluk seviyesine ulaşana kadar eski sistemle beraber çalıştırılmasına devam edilir. Bu şekilde paralel işletimin mümkün olmadığı durumlarda ise, değiştirilmiş veya yeni geliştirilmiş sistem belirli bir olgunluk seviyesine ulaşana kadar eski sistem veri kayıpsız olarak devreye alınabilir halde tutulur.

Bilgi sistemlerinin kullanımı ile ilgili gerekli eğitim materyalleri oluşturulur.

3. İŞ SÜREKLİLİĞİ VE BİLGİ SİSTEMLERİ SÜREKLİLİK PLANI

Şirket' in iş süreçleri bakımından kritik olan veriler Şirket'in muhasebe kayıtlarıdır. Şirket'in ilgili mevzuat uyarınca asgari olarak ayda bir kere yapması gereken raporlamalar bulunmaktadır. Birincil sistemlerde oluşabilecek bir arıza ve veri kaybı halinde, yedek verilerin azami bir ay içinde devreye alınması ve Şirket'in raporlama yapabilecek duruma geri dönmesi gerekmektedir.

İş sürekliliğinin aksamaması bakımından Şirketin muhasebe kayıtları haftalık olarak yedeklenir. Bunun dışında kalan bilgiler ise ayda bir kere yedeklenir. Birincil sistemlerde bir arıza ve veri kaybı olması durumunda, yedek alınan veriler sistemlere yüklenir. Varsa en son yedek alma tarihinden sonraki dönemde gerçekleşen muhasebe işlemlerinin kayıtları evrak üzerinden manuel olarak verinin bütünlüğü sağlanır.

4. VERİ YEDEKLEMESİ VE ALTERNATİFLİ KURTARMA SÜREÇ VE PROSEDÜRLERİ

Şirket'in birincil ve ikincil sistemlerini yurt içinde bulundurması zorunludur. Şirket'in birincil sistemleri Şirket merkezinde bulundurulur. İkincil sistemler (birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve mevzuatta tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistem yedekleri) ise taşınabilir medyalar üzerinde oluşturulmalı ve birincil sistemlere zarar verebilecek felaketlerden etkilenmeyecek kadar uzakta ve güvenli bir yerde saklanmalıdır. Yedekleme medyaları etiketlenmeli ve hangi medyada hangi yedeğin bulunduğuna dair kayıtlar tutulmalıdır. Yedekleme bilgisine uygun seviyede fiziksel ve çevresel koruma sağlanmalıdır. Gizliliğin önemli olduğu durumlarda yedeklemelerin kriptolu olarak alınması göz önünde bulundurulmalıdır.

Yedekleme işlerine ait kayıtlar ayrıca tutulmalı, başarısız olan yedekleme işleri takip edilmeli ve yedeği alınamamış verinin yedeği alınmalıdır.

Yedeklenmiş verinin düzenli aralıklarla geri döndürme testi yapılmalıdır. Yedeklemenin türü (tam yedekleme/değişen kayıtların yedeklenmesi), yedeklemenin sıklığı iş gereklerine, güvenlik gereksinimlerine ve bilginin kritiklik derecesine göre belirlenmelidir.

5. BİLGİ SİSTEMLERİ GÜVENLİĞİNE İLİŞKİN SÜREÇ VE PROSEDÜRLER

a. Fiziksel ve Çevresel Güvenlik

Çalışan personele ait şahsi dosyalar kilitli dolaplarda muhafaza edilmeli ve dosyaların anahtarları kolay ulaşılabilir bir yerde olmamalıdır. Gizlilik ihtiva eden yazılar kilitli dolaplarda muhafaza edilmelidir. İmha edilmesi gereken yazılar bekletilmeden imha edilmelidir. Personel dışındaki kişilerin ofislere girişleri kontrol edilmeli ve bilgi kaynaklarının olduğu mekanlara personel eşliği haricinde girişlerine izin verilmemelidir. Şirket personeli veya dışarıdan hizmet alınan kuruluşların çalışanları için "ihtiyacı kadar bilme" prensibi uygulanmalıdır.

b. Ekipman Güvenliği ve Temiz Masa Kuralları

Hassas bilgiler içeren evraklar, bilgi ve belgelerin masa üzerinde kolayca ulaşılabilir yerlerde ve açıkta bulunmaması gereklidir. Bu bilgi ve belgelerin kilitli yerlerde muhafaza edilmesi gerekmektedir. Personelin kullandığı masaüstü veya dizüstü bilgisayarlar iş sonunda ya da masa terkedilecekse ekran kilitlenmelidir. Bu işlem Windows + L tuşuna basılarak yapılabilir. Sistemlerde kullanılan şifre, telefon numarası ve T.C kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulunmamalıdır. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilmeli, bilginin geri dönüşümü ya da yeniden kullanılabilir hale geçmesinin önüne geçilmelidir. Faks makinelerinde gelen giden yazılar sürekli kontrol edilmeli ve makinede yazı bırakılmamalıdır. Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler (sunucu), PC'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalıdır.

Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır. Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir. Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir. Özel koruma gerektiren ekipman izole edilmiş olmalıdır. Bilgi işlem araçlarının yakınında yeme, içme ve sigara içilmesi engellenmelidir.

Ekipmanın bakımı doğru şekilde yapılmalıdır. Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır. Bakım sadece yetkili personel tarafından yapılıyor olmalıdır. Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır. Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir. İçindeki hassas bilgiler silinmelidir. Ekipman sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır. Üretici garantisi kapsamındaki ürünler için garanti süreleri kayıt altına alınmalı ve takip edilmelidir. Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir. Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyulmalıdır. Evden çalışma ile ilgili tedbirler alınmalıdır. Cihazların sigortaları, tesis dışında korumayı da kapsamalıdır.

Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir. Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format işlemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.

c. İşletim Sistemi Güvenliği

Son kullanıcı düzeyinde hangi işletim sistemini kullanacağına karar verilmeli ve bu işletim sistemine uygun yazılım donanım sistemleri kullanılmalıdır. İşletim sistemlerinin güncel ve güvenli olması için yama yönetimi yapılmalıdır. Envanter haricindeki donanımların kurum bilgisayarlarında kullanımı engellenmelidir.

d. Son Kullanıcı Güvenliği

Son kullanıcılar sistemlere, etki alanları dâhilinde kendilerine verilmiş kullanıcı adı ve şifreleri ile bağlanmalıdır. Son kullanıcılar, yetkileri dâhilinde sistem kaynaklarına ulaşabilmeli ve internete çıkabilmelidir. Son kullanıcıların aktiviteleri, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglanarak kayıt altına alınmalıdır. Güvenlik zafiyetlerine karşı, son kullanıcılar kendi hesaplarının ve/veya sorumlusu oldukları cihazlara ait kullanıcı adı ve şifre gibi kendilerine ait bilgilerin gizliliğini korumalı ve başkaları ile paylaşmamalıdır. Son kullanıcılar bilgisayarlarındaki ve sorumlusu oldukları cihazlardaki bilgilerin düzenli olarak yedeklerini almalıdır. Son kullanıcılar, güvenlik zafiyetlerine sebep olmamak için, bilgisayar başından ayrılırken mutlaka ekranlarını kilitlemelidir. Son kullanıcılar, bilgisayarlarında ya da sorumlusu oldukları sistemler üzerinde USB flash bellek ve/veya harici hard disk gibi taşınabilir medya bırakmamalıdır. Son kullanıcılar, mesai bitiminde bilgisayarlarını kapatmalıdır. Kullanıcı bilgisayarlarında, güncel anti virüs bulunmalıdır.

e. Parola Güvenliği

Parolalar en az 8 karakterden oluşmalıdır. Harflerin yanı sıra, rakam ve "?, @, !, #, %, +, -, *, %" gibi özel karakterler içermelidir. Büyük ve küçük harfler bir arada kullanılmalıdır. Kişisel bilgiler gibi kolay tahmin edilebilecek bilgiler parola olarak kullanılmamalıdır (örneğin 12345678, qwerty, doğum tarihi, bir yakının adı, soyadı gibi). Sözlükte bulunabilen kelimeler parola olarak kullanılmamalıdır. Çoğu kişinin kullanabildiği aynı veya çok benzer yöntem ile geliştirilmiş parolalar kullanılmamalıdır. Personelin gönderdiği maillerde, hiçbir şekilde yönetici, kullanıcı gibi hesap şifreleri bulundurulmamalıdır. Taşınabilir ortam, cihaz ve iletişim hatlarında iletilen hassas bilginin korunması için şifreleme mekanizmalarının kullanılmalıdır.

f. İnternet ve E-posta Güvenliği

Kullanıcıya resmi olarak tahsis edilen e-posta adresi, kötü amaçlı ve kişisel çıkar amaçlı kullanılamaz. İş dışı konulardaki haber grupları kurumun e-posta adres defterine eklenemez. Kurumun e-posta sunucusu, kurum içi ve dışı başka kullanıcılara SPAM, phishing mesajlar göndermek için kullanılamaz. Kurum içi ve dışı herhangi bir kullanıcı ve gruba; küçük düşürücü, hakaret edici ve zarar verici nitelikte e-posta mesajları gönderilemez. İnternet haber gruplarına mesaj yayımlanacak ise, kurumun sağladığı resmi e-posta adresi bu mesajlarda kullanılamaz. Ancak iş gereği üye olunması yararlı internet haber grupları için yöneticisinin onayı alınarak Kurumun sağladığı resmi e-posta adresi kullanılabilir. Hiçbir kullanıcı, gönderdiği e-posta adresinin kimden bölümüne yetkisi dışında başka bir kullanıcıya ait e-posta adresini yazamaz. E-posta gönderiminde konu alanı boş bir e-posta mesajı göndermemelidir. Konu alanı boş ve kimliği belirsiz hiçbir e-posta açılmamalı ve silinmelidir. E-postaya eklenecek dosya uzantıları ".exe", ".vbs" veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, dosyalar sıkıştırılarak (zip veya rar formatında) mesaja eklenmelidir. Gizli bilgi, gönderilen mesajlarda yer almamalıdır. Bunun kapsamı içerisine iliştirilen öğeler de dâhildir. Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere özen gösterilmelidir. Zincir mesajlar ve mesajlara iliştirilmiş her türlü çalıştırılabilir dosya içeren e-postalar alındığında başkalarına iletilmeyip, üst yönetime haber verilmelidir. Spam, zincir, sahte vb. zararlı olduğu düşünülen e-postalara yanıt verilmemelidir. Kullanıcı, kullanıcı kodu/parolasını girmesini isteyen e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın üst yönetime haber vermelidir. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru olduğu düşünülen e-postalar üst yönetime haber verilmelidir. Kullanıcı, kendisine ait e-posta parolasının güvenliğinden ve gönderilen e-postalardan doğacak hukuki işlemlerden sorumlu olup, parolasının kırıldığını fark ettiği anda üst yönetime haber vermelidir.

g. Yazılım ve Donanım Güvenliği

Kurum içerisinde kullanılan tüm bilgisayarların zararlı yazılımlara karşı en güncel anti virüs yazılımına sahip olmalıdır. Bilgisayarlarda kullanılan anti virüs yazılımları düzenli olarak güncellenmelidir. Bilgisayarların üzerinde kullanılan işletim sistemleri düzenli olarak güncelleştirilmelidir. Bilgisayarlar üzerinde korsan yazılımlar bulundurulmamalıdır. Kurum için geliştirilen uygulamalar ve satın alınan yazılımlar, güvenlik zafiyetlerine neden olmamak için en son stabil yamalara ve güncelleştirmelere sahip olmalıdır.

Kuruma ait sistemler dışarıdan gelebilecek saldırılara karşı, güncel teknolojilere sahip donanımsal firewall cihazları ile korunmalıdır. Kurum çalışanlarının internete çıkışlarının kontrol edilerek, zararlı ve kurum politikasına uymayan sitelere erişimlerinin engellenmesi için proxy cihazları ile korunmalıdır. Kuruma ait uygulamaların güvenli bir şekilde çalışması ve uygulamalara gelebilecek saldırıların engellenmesi için Web Application Firewall (Web Uygulama Güvenlik Duvarı) ile korunmalıdır. Kurumda kullanılan bütün güvenlik cihazlarının konfigürasyon yedekleri periyodik olarak alınmalı, doğru şekilde etiketlenerek saklanmalıdır. Kurumda kullanılan bütün sistem ve güvenlik donanımları, kurumun ihtiyaçlarına bağlı olarak sadece izin verilen erişimlere göre konfigüre edilmelidir.

h. Kaydedilebilir Taşınır Materyaller Güvenliği

Şirkete ait hiçbir veri CD, USB, taşınabilir disk ve benzeri materyale kopyalanması kesinlikle yasaktır. Bunun için gereken güvenlik önemleri alınmıştır. Taşınacak veri eğer USB disk ile taşınacaksa bu usb diskin tehdit unsuru olan bir yazılım içermediğine emin olunmalıdır. USB disk biçimlendirildikten sonra veri kopyalanmalıdır. Veri ister USB disk, isterse de CD, DVD ortamında taşınsın kesinlikle şifrelenmelidir. USB diskleri bilgisayardan çıkartılırken önce aygıtı düzenli şekilde çıkart komutu vererek bağlantısı kesilmelidir. Harici taşınabilir disklerin içi mekanik yapıya sahip olduğundan, dolayı darbelere karşı çok hassastır. Bu nedenle kullanırken ve taşırken dikkat edilmelidir. Özellikle hard diskler taşınırken koruyucu kılıflar içerisinde taşınmalıdır. CD ve DVD'lerde veri saklamak için ise kaliteli medyalar kullanılmalı, düşük hızla yazdırılmalı, alt yüzeye mümkün olduğunca temas edilmemeli, nemli olmayan, ışık almayan ortamlarda ve çok fazla sıkıştırmadan saklanmalıdır. Kötü amaçlı kimselerin bilgilere ulaşmasını engellemek için taşınabilir materyaller güvenilir şekilde muhafaza edilmeli, gerekirse kilitli dolaplarda veya çelik kasalarda saklanmalıdır. Taşınır materyaller çalışma masasında veya bilgisayarda güvensiz şekilde bırakılmamalıdır. Gerekmediği sürece dışarıya çıkartılmamalı, kaybolma riskine karşı tedbirli olunmalıdır.

6. BİLGİ SİSTEMLERİ RİSK YÖNETİMİ SÜREÇ VE PROSEDÜRLERİ

Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak aşağıdaki hususlar değerlendirmeye katılır:

a) Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda gelişmelere uymamanın olumsuz sonuçları, gelişmelere uyma konusundaki zorluklar ve yasal mevzuatın değişebilmesi,
b) Bilgi sistemleri kullanımının öngörülemeyen hatalara ve hileli işlemlere zemin hazırlayabilmesi,
c) Bilgi sistemlerinde dış kaynak kullanımından dolayı dış kaynak hizmeti veren kuruluşlara bağımlılığın oluşabilmesi,
d) İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi,
e) Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

Bilgi sistemlerine ilişkin risk analizi yapılır. Yılda en az bir defa veya bilgi sistemlerinde meydana gelebilecek önemli değişikliklerde tekrarlanır.

Bilgi sistemlerinin teknik açıklarına ilişkin bilgi, zamanında elde edilir ve şirketin bu tür açıklara karşı zafiyeti değerlendirilerek, riskin ele alınması için uygun tedbirler alınır.

Şirket'in bilgi sistemleri, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez sızma testine tabi tutulur.

Sızma testinde sermaye piyasası mevzuatında belirlenen usul ve esaslar uygulanır.

7. BİLGİ GÜVENLİĞİ POLİTİKASI ESASLARI

Şirket kurumsal bilgiyi son derece değerli bir varlık olarak kabul etmektedir. Bilgi, iş faaliyetlerimizin sürdürülebilmesi açısından kritik önem taşır ve uygun bir şekilde korunması gerekir. Şirket kurumsal bilginin gizliliğini, bütünlüğünü ve gerektiğinde erişilebilir olmasını ve bu unsurlarla ilgili ortaya çıkabilecek risklerin etkilerini en aza indirmeyi amaçlar. Bu çerçevede;

- ✓ **Gizlilik, bilginin sadece yetkili kişiler tarafından erişilebilir olması,**
- ✓ **Bütünlük, bilginin yetkisiz değişimlerden korunması ve değiştirildiğinde farkına varılması,**
- ✓ **Erişilebilirlik, bilginin yetkili kullanıcılar tarafından gerektiğinde erişilebilir olmasıdır.**
- ✓ **Şirkete ait tüm bilgi ve kişisel veriler kullanıcı PC'lerinde değil ilgili sunucu ve sistemler üzerinde barındırılmaktadır. Bu verilerin kullanıcı bilgisayarında taşınması veya aktarılmaması gerekmektedir**.

Şirket'in tüm yönetici ve çalışanları ile dışarıdan hizmet aldığı kuruluşların bu hizmeti sağlamakla görevlendireceği çalışanları, bilgi güvenliğini sağlamak için gereken özen ve basireti göstermek zorundadır. Şirket ve dışarıdan hizmet alınan kuruluş personeli görevlerini yerine getirirken, Şirket'e ait bilgilerin yetkili ellerde kalmasını ve Şirket bünyesinde korunmasını gözetecek biçimde hareket etmekten sorumludur. Bu çerçevede, Şirket'in bilgi işlem altyapısını kullanan ve bilgi kaynaklarına erişen herkes;

- ✓ **Kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kurum bilgilerinin gizliliğini korumalıdır.**
- ✓ **Bilgi güvenliği ihlali tespit etmesi durumunda bunu üst yönetime raporlamalıdır.**
- ✓ **Bilgi kaynaklarını Şirket içinden dahi olsa yetkisiz kişiler ile paylaşmamalıdır.**
- ✓ **Şirket'in bilişim kaynaklarını yasalara ve yönetmeliklere aykırı faaliyetler amacı ile kullanmamalıdır.**

Şirket tüm çalışanların, bilgi güvenliği konularıyla ilgili uygun bilinçlenme düzeyinin oluşmasını sağlayacak uygun eğitimleri almalarını temin edecek ve genel olarak bilgi güvenliği olaylarının ele alınmasında rehberlik edecektir.

Şirket yöneticileri, bilgi güvenliği politikasına uyumun sağlanması için gerekli tedbirleri almak ve sistemi gözetlemekten birinci derece sorumludur.

Uyumsuzluk ve Disiplin Uygulamaları

Bu politika hükümlerine aykırı hareket eden, bilgi güvenliği kurallarını ihlal eden veya gerekli özen ve sorumluluğu göstermeyen tüm çalışanlar hakkında, ihlalin niteliği ve ağırlığı dikkate alınarak yürürlükte bulunan **Disiplin Prosedürü** hükümleri uygulanır. Bu kapsamda, ilgili mevzuat, şirket iç düzenlemeleri ve iş sözleşmeleri çerçevesinde gerekli idari ve/veya disiplin yaptırımları tesis edilir; gerekli görülmesi hâlinde konu, ilgili birimlere ve yetkili mercilere intikal ettirilir. Bu uygulamalar, bilgi güvenliğinin sürekliliğini sağlamak, kurumsal varlıkları korumak ve mevzuata uyumu temin etmek amacıyla yürütülür.