ADESE GAYRİMENKUL YATIRIM ANONİM ŞİRKETİ

BİLGİ SİSTEMLERİ YÖNETİM POLİTİKASI

1. Amaç

Bu politikanın amacı, Adese Gayrimenkul Yatırım A.Ş. (‘’ Adese ‘’) nezdinde, bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik usul ve esasların belirlenmesi; bilgi güvenliği risklerinin yönetilmesi ve VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği’ne tam uyumun sağlamasıdır.

Bu Politika bağlamında “bilgi varlığı”, Adese’nin 6362 sayılı Sermaye Piyasası Kanunu’ndan ve bu Kanuna ilişkin alt düzenlemelerden kaynaklanan hizmet ve görevlerini yerine getirmeleri esnasında kullandıkları veri ile bunların üretildiği, işlendiği, iletildiği ve saklandığı donanım ve yazılım unsurlarıdır.

Bilgi Güvenliği Politikamızın en temel hedefi, bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini güvence altına alarak, Şirket’in operasyonel verimliliğini artırmak ve iş süreçlerini kesintiye uğratmadan devam ettirmektir.

2. Kapsam

Bu politika, Adese bünyesinde kullanılan tüm bilgi sistemleri, veri tabanları, altyapı, uygulamalar, hizmet sağlayıcılar, yazılım ve donanım çözümleri, Şirket içi çalışanlar, taşeronlar ve üçüncü taraf hizmet sağlayıcıları için geçerlidir.

3. Politika Esasları

Adese nezdinde uygulanacak olan Bilgi Güvenliği Politikası aşağıdaki alt başlıklar ile detaylandırılmıştır:

3.1 Bilgi Güvenliği Yönetimi

Adese, bilgi güvenliğini öncelikli bir iş hedefi olarak kabul eder. Şirketin üst yönetimi, yasal düzenlemelere, sözleşmelere ve endüstri standartlarına uygun hareket ederek, aşağıdaki hususları sağlamak için gerekli adımları atar:

- Gizlilik, bütünlük ve erişilebilirlik ilkelerine dayalı güvenlik önlemlerinin alınması,
- Risk yönetimi süreçlerinin oluşturulması ve düzenli olarak gözden geçirilmesi,
- İç denetim ve dış denetimlerle bilgi güvenliği önlemlerinin etkinliğinin izlenmesi,
- Sürekli iyileştirme süreçlerinin uygulanması.
- İşbu Politikanın her yıl gözden geçirilmesi ve gerekli hallerde güncellenmesi.

3.2 Risk Yönetimi ve Kontroller

Adese, bilgi güvenliği kontrollerinin etkin bir şekilde hayata geçirilmesi için bilgi teknolojileri varlıklarının risk değerlendirmelerinin ve maruz kaldıkları riskler için kontrol oluşturma çalışmalarının yapılması kaçınılmazdır. Bu kapsamda:

- Düzenli olarak risk değerlendirme çalışmalarının yapılması ve takip edilmesi konusunda sorumluluklar belirlenir ve hayata geçirilir.
- Bilgi güvenliği riskleri, düzenli olarak tanımlanacak, değerlendirilecek ve önceliklendirilecektir. Bilgi güvenliği risklerinin tanımlanması, değerlendirilmesi ve işlenmesi, kurumun risk yönetimi kapsamında ele alınır.
- Risklere karşı alınacak önlemler, yönetim düzeyinde izlenecek ve uygulamada yeterlilik sağlanacaktır.
- Yönetim kurulu, yıllık risk değerlendirmeleri ve periyodik kontrol süreçlerini gözden geçirecek ve iyileştirme önerileri üzerinde karar verecektir.
- Risk analizleri, şirketin kritik iş süreçleri ve bilgi sistemleri üzerinde düzenli aralıklarla yapılacaktır.

3.3 Erişim Kontrolü ve Kullanıcı Yönetimi

- Adese, bilgi sistemlerine erişim, kullanıcıların görev ve sorumluluklarına göre sınıflandırılacak ve yalnızca yetkili kişiler tarafından yapılabilecektir.
- Sistemlere erişimde çok faktörlü kimlik doğrulama (MFA), tüm kritik sistemlerde zorunlu hale getirilmiştir. MFA altyapısı kapsamında, SecNap MFA uygulaması ve FortiToken doğrulama mekanizmaları kullanılmaktadır.
- Kullanıcı hesapları, güvenli parola yönetimi ve rol bazlı erişim kontrolleri ile yönetilir.
- Kullanıcı erişim hakları, düzenli olarak gözden geçirilmekte ve gereksiz erişimler derhal iptal edilmektedir.

3.3.1. Parola Yönetimi

Adese, bilgi sistemleri ortamlarına erişirken kullanılan şifrelerin standartlara uygun biçimde oluşturulması, korunması, kullanılması ve değiştirilmesi, kullanıcılara tanımlanan şifreler konusunda çalışanların bilgilendirilmesi ve şifre işlemlerinin Şirket'in riskini en aza indirecek en güvenli şekilde yapılmasını sağlamak amacı gözetilir.

3.3.2. E-posta Güvenliği, İnternet Kullanımı ve Ağ Erişimi

- E-posta, Şirket'in en önemli ve kullanılması kaçınılmaz iletişim kanallarından biridir. Bunun yanı sıra e-posta, basitliği ve hızı nedeni ile yanlış veya gereğinden fazla kullanıma açık bir kanaldır. Bu amaçla e-posta adresi oluşturma ve tanımlama ile bu e-posta hesaplarının kullanımına yönelik kurallar ile e-posta virüs güvenliğine düzenli gözden geçirmeler yapılır. Kurumsal e-posta ve ofis uygulamaları Microsoft 365 platformu üzerinden sunulmaktadır. Kullanıcı verileri güvenli, ölçeklenebilir ve bulut tabanlı bir altyapı üzerinde yönetilmektedir.
- İnternetin uygun olmayan kullanımı, Kurum'un yasal yükümlülükleri, kapasite kullanımı ve profesyonel imajı açısından istenmeyen sonuçlara neden olabilir. Bilerek ya da bilmeden, bu türden olumsuzluklara neden olunmaması amacı ile İnternet'in kurallara, etik ve yasalara uygun kullanımı sağlanır.
- Ağ erişimlerinin kontrolü amacıyla yerli yazılım olan SecNap NAC çözümü kullanılmaktadır.
- Kullanıcı ve cihaz bazlı erişim politikaları uygulanmakta, yetkisiz veya uyumsuz cihazların ağa erişimi engellenmektedir.

3.3.3. Log Yönetimi

Adese, tüm kritik sistem ve uygulamalarının iz kayıtları saklanmakta, izlenmekte ve analiz edilmektedir. Bu kapsamda, ağ ve güvenlik bileşenlerine ait loglar FortiAnalyzer üzerinden merkezi olarak toplanmakta ve analiz edilmektedir.

- FortiAnalyzer sayesinde:
    - Firewall ve ağ cihazlarına ait olay kayıtları merkezi olarak izlenmekte,
    - Güvenlik olayları geriye dönük olarak analiz edilebilmekte,
    - Denetim ve raporlama süreçleri desteklenmektedir.
- Merkezi loglama altyapısı, olay müdahale ve adli analiz süreçlerine katkı sağlamaktadır.

3.3.4. Kimlik Yönetimi

Adese nezdinde Kimlik Yönetimi (Identity Management – IDM):

- Kurumsal kimlik ve erişim yönetimi Microsoft Active Directory (AD) üzerinden sağlanmaktadır.
- Kullanıcı hesapları, grup politikaları ve yetkilendirmeler merkezi olarak yönetilmektedir.

Ayrıcalıklı Erişim Yönetimi (PAM) için ise:

- FortiPAM (Fortinet PAM) çözümü kullanılmaktadır.

- Yetkili erişimler kontrol altına alınmakta ve kayıt altına alınmaktadır.

3.4 Yedekleme ve Veri Koruma

Adese nezdinde bilgi sistemleri, iş sürekliliği önceliklerine uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir. Bu kapsamda yedekleme çizelgesi hazırlanır, üst yönetime onaylatılır ve güncelliği sağlanır. Yedeklerin en az bir kopyası farklı coğrafi bir konumda saklanır. Yedeklerin güvenliğine ilişkin gerekli önlemler alınır. Bu kapsamda,

- İş sürekliliğini sağlamak amacıyla veriler 3 farklı lokasyonda tutulmaktadır.
- Bu lokasyonlardan en az biri bulut ortamı olacak şekilde felaket kurtarma senaryoları uygulanmaktadır.
- Olası kesinti ve felaket durumlarında hizmetlerin devamlılığı hedeflenmektedir.

4. Bilgi Güvenliği İhlalleri ve Olay Müdahale

Aşağıdaki durumlardan en az birinin gerçekleşmesi durumunda Bilgi Güvenliği Politikasının çalışanlar tarafından ihlal edildiği sonucuna varılır:

a. Kasten ya da ihmal sonucu Bilgi Güvenliği Politikasına ve/veya ilgili alt politikalar, prosedürler, talimatlar ve standartlarda açıkça belirtilmiş maddelere karşı hareket etmek,
b. Şirket'in itibarını riske atmak,
c. Şirket'in bilgilerini ve bilgi güvenlik sistemini tehlikeye atarak, anılan şirketleri fiili ve olası iş kaybına maruz bırakmak,
d. Şirket'in bilgilerini yetkisiz bir şekilde kullanmak, ifşa etmek, değiştirmek, tahrip etmek ve/veya bu bilgileri izinsiz bir şekilde üçüncü kişilerle yazılı/elektronik olarak herhangi ortamda paylaşmak,
e. Şirket'in bilgi varlıklarını yasal olmayan bir amaç için kasten ya da ihmal sonucu kullanmak.

Şirket'in, Bilgi Güvenliği Politikasının ihlali durumunda bu ihlalin ciddiyetine göre hareket etme hakkını saklı tutar; ancak işbu Politika'ya uymama veya kasıtlı Politika ihlalleri, disiplin cezası, yazılı kınama, işten çıkarma, hukuk muameleleri ve/veya cezai kovuşturmalar dâhil olmak üzere bunlarla sınırlı olmayan eylemlerle sonuçlanabilir. İhlalin ciddiyetine göre, çalışanın sistemlere erişim haklarını ve ilgili sorumlulukları askıya alınabilir.

Ek olarak;

- Bilgi güvenliği ihlali durumunda, olay müdahale prosedürleri uygulanacak ve ihlalin kaynağı hızla tespit edilerek gerekli düzeltici önlemler alınacaktır.

- Olay müdahale planları, ilgili tüm ekiplerle birlikte test edilecek ve en hızlı şekilde sorun çözülmesi sağlanacaktır.

- Şirket çalışanları veya üçüncü taraf kullanıcıları, bir güvenlik açığıyla karşılaştıklarında olası güvenlik olaylarını engellemek amacıyla, durumu mümkün olduğu kadar kısa sürede rapor etmelidir. Tüm personel, kullandığı sistemlerin ve uygulamaların durum bilgilerine sahip olmalı ve tüm yetkisiz kullanım ve şüpheli durumları rapor etmek için hazır olmalıdır.

5. Bilgi Güvenliği Eğitimi ve Farkındalık

Şirket çalışanlarının bilgi güvenliğine yönelik farkındalıklarını arttırabilmek bu Politikanın temel amaçlarından biridir. Bu nedenle İnsan Kaynakları eğitim programlarına entegre bir şekilde, Kurum çalışanlarına yönelik işe girişte ve çeşitli dönemlerde bilgi güvenliği farkındalığı arttırma ve bilinçlendirme eğitimleri düzenlenir. Bu eğitimler çerçevesinde Kurum, bilgi güvenliği çerçevesinin ve standartlarının çalışanlara aktarılması, güvenlik politika ve standartların farkında olunması ve politikalardaki rol ve tanımların bilinmesi ve sahiplenilmesini amaçlar.

Adese, bilgi güvenliği kültürünü tüm organizasyona yaymak için aşağıdaki adımları atar:

- Yıllık bilgi güvenliği eğitimleri düzenlenecek ve çalışanların bilgi güvenliği bilinci sürekli artırılacaktır.

- İç ve dış denetimler ile bilgi güvenliği uyum seviyeleri ölçülecek ve bu bulgular doğrultusunda eğitimler güncellenerek yenilenmeye gidilecektir.

- Eğitimlere katılım zorunlu olacak ve sertifika verilerek katılım sağlanacaktır.

- Çalışanların, bilgi güvenliği ihlallerini gözlemlemeleri ve raporlamaları teşvik edilecektir.

6. Bilgi Sistemleri ve Altyapı Güvenliği

6.1 Altyapı Güvenliği

- Şirket altyapısı, güncel güvenlik yamaları ve önlemleriyle korunacaktır.

- Zararlı yazılımlara karşı koruma sağlamak için anti-virüs yazılımları ve güvenlik duvarları aktif hâlde olacaktır.

- Fiziksel güvenlik de sağlanacak ve yalnızca yetkili personel tarafından erişim sağlanacaktır.

- Veri şifreleme uygulamaları, şirket verilerinin korunmasını sağlamak amacıyla tüm kritik verilerde kullanılacaktır.

6.2 İş Sürekliliği ve Felaket Kurtarma

- İş sürekliliği planları hazırlanacak ve felaket kurtarma prosedürleri her yıl test edilecektir.
- Kritik iş süreçlerine ilişkin, kabul edilebilir kesinti süreleri (RTO) ve veri kaybı toleransları (RPO) belirlenecek ve uyumlu bir şekilde çalışacaktır.
- Sürekli iyileştirme, iş sürekliliği planlarında ve felaket kurtarma planlarında periyodik olarak yapılacaktır.

6.3 Denetim ve İzleme

- Dış denetimler ve iç denetim süreçleri düzenli olarak gerçekleştirilecektir.
- Sızma testleri (Penetration Testing) ve güvenlik testleri, potansiyel açıkların tespit edilmesi ve bunların giderilmesi amacıyla yapılacaktır.
- Erişim ve kullanım logları düzenli olarak izlenecek ve herhangi bir şüpheli faaliyet hemen raporlanacaktır.
- Bilgi sistemleri güvenliğine ilişkin kontrollerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hususunda üst yönetime rapor veren, bilgi sistemleri iç kontrol, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarının herhangi birinde yeterli teknik bilgiye ve en az 5 yıl tecrübeye sahip bir bilgi güvenliği sorumlusu belirlenir.

7. Uyumluluk ve Yaptırımlar

- Adese de bu politika ve prosedürlere uymayan çalışanlar, uyarma, kınama veya sözleşme feshi gibi yaptırımlara tabi olacaktır.
- Üçüncü taraflar, yazılım ve hizmet sağlayıcılar ile yapılacak sözleşmelerde bilgi güvenliği gereklilikleri net bir şekilde belirtilecektir.
- Yasal uyumluluk, yerel ve uluslararası düzeyde, sürekli izlenecek ve her yıl güncel mevzuata uygunluk test edilecektir.

8. Gözden Geçirme ve Güncelleme

- Bu politika, her yıl Adese'nin üst yönetimi ile Bilgi Güvenliği Sorumlusu tarafından gözden geçirilecek ve iş ihtiyaçları, değişen tehdit ve risklere göre güncellenir.
- Politika, teknolojik değişiklikler, yasal düzenlemeler veya önemli sistem değişiklikleri durumunda önceden gözden geçirilecek ve güncellenmiş versiyonu ilgili tüm taraflara duyurulacaktır.

- İşbu Bilgi Güvenliği Politikasının güncellenmesi için yeter şartlar aşağıda sıralanmıştır:

a) Sistem bileşenlerinde büyük değişiklik olması,
b) Yeni tipte güvenlik ihlallerinin çıkması,
c) Mevzuatta, kurumsal süreçlerde ya da işletim talimatlarında değişiklik yapılması,
d) Güvenlik gereksinimlerinde değişiklik olması,
e) Güvenlik ihlalleri,
f) Bilgi Teknolojileri Birimlerinin ihtiyaç duyduğu diğer tüm haller

Bilgi Güvenliği Politikası gözden geçirilirken aşağıda listelenen hususlar özellikle değerlendirilmelidir:

a) Mevcut politikanın etkinliği ve yeterliliği,
b) Tercih edilen güvenlik önlemlerinin ve korunan varlıkların değerleri,
c) Teknolojideki değişiklikler

9. Yürürlük

- Bu politika, Yönetim Kurulu tarafından onaylanma tarihinde yürürlüğe girer.