Orjin Maslak Gayrimenkul Yatırım İnşaat A.Ş. ("**Şirket**") tarafından hazırlanan işbu Bilgi Güvenliği Politikası, Şirket'in faaliyetlerini sürdürürken sahip olduğu bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunmasını stratejik bir öncelik olarak kabul etmektedir. Bu politika; Şirket'imizin yürüttüğü gayrimenkul, gayrimenkul projeleri ve gayrimenkule dayalı haklara yatırım faaliyetleri ile bu faaliyetleri destekleyen teknoloji ve veri analitiği süreçlerinde kullanılan bilgi varlıklarının korunmasına yönelik temel prensipleri ortaya koymayı; bilgi sistemlerinin güvenli şekilde kurulması, işletilmesi, yönetilmesi ve kullanılmasını; bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasını, bilgi güvenliği risklerinin etkin şekilde yönetilmesini ve gerekli kontrol mekanizmalarının tesis edilmesini amaçlamaktadır.

KAPSAM

Bu politika aşağıdaki faaliyetleri ve varlıkları kapsar:

- Gayrimenkul, gayrimenkul projeleri ve gayrimenkule dayalı haklara yatırım faaliyetleri,
- Bu faaliyetleri destekleyen teknoloji ve veri analitiği süreçleri,
- Yazılım ve donanım altyapıları,
- Sistem odası ve ilgili bilgi işlem altyapıları,
- Elektronik, fiziksel ve sözlü ortamdaki tüm bilgi varlıkları,
- Şirket adına işlenen kişisel veriler ile bu verilerin işlendiği tüm ortamlar,
- Şirket çalışanları, yöneticileri, danışmanları, tedarikçileri ve bilgi varlıklarına erişimi bulunan ilgili taraflar.

REFERANS ALINDAN DÜZENLEMLER VE UYUM

Şirket, bilgi güvenliği ve bilgi sistemleri yönetimi bakımından tabi olduğu mevzuat ve düzenlemelere uyar. VII-128.10 sayılı Bilgi Sistemleri Yönetimine İlişkin Usul ve Esaslar Tebliği'nde ("**Tebliğ**") yer alan ilke ve standartlar, Şirket bakımından uygulanabilir oldukları ölçüde işbu politikanın hazırlanmasında referans alınmıştır. Şirket, bilgi sistemlerinin gizlilik, bütünlük ve erişilebilirlik ilkeleri doğrultusunda yönetilmesine, bilgi güvenliği risklerinin etkin şekilde yönetilmesine ve gerekli kontrol mekanizmalarının tesis edilmesine azami özen gösterir.

İLKELER

Şirket, Bilgi Güvenliği Yönetim Sistemi kapsamında aşağıdaki ilkeleri benimser:

- Bilgi sistemlerinin yönetim, kurumsal yönetim uygulamalarının bir parçası olarak ele alınır. Bilgi sistemlerine ilişkin stratejilerin Şirket'in iş hedefleriyle uyumlu olması; bilgi sistemlerinin güvenli, etkin, doğru ve sürekli şekilde işletilmesi ve bu amaçla gerekli insan kaynağı, teknoloji, finansal kaynak ve organizasyonel desteğin sağlanması esastır.
- Bilgi varlıkları; gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olarak korunur. Bilgi varlıklarının kritiklik ve hassasiyet düzeyleri belirlenir ve uygulanacak güvenlik önlemleri bu sınıflandırmaya uygun olarak tesis edilir.
- Bilgi sistemlerine ilişkin risklerin belirlenmesi, ölçülmesi, izlenmesi, işlenmesi ve raporlanmasına yönelik risk yönetimi süreç ve prosedürleri oluşturulur ve güncel tutulur. Risk analizleri yılda en az bir defa ve bilgi sistemlerinde meydana gelecek önemli değişikliklerde tekrarlanır; risklerin azaltılmasına yönelik iyileştirici faaliyetler belirlenerek takip edilir.
- Bilgi güvenliği süreçlerinin işletilmesi için gerekli roller, sorumluluklar ve görev tanımları belirlenerek yazılı hale getirilir. Bilgi sistemleri üzerindeki hata, eksiklik ve kötüye kullanım risklerinin azaltılması amacıyla görevler ayrılığı ilkesi uygulanır; kritik işlemlerin tek bir personele veya dış hizmet sağlayıcıya

bağımlı olmaması gözetilir. Görevlerin uygun şekilde ayrılmasının mümkün olmadığı durumlarda telafi edici kontroller tesis edilir.

- Bilgi sistemlerinin yönetimine ilişkin kontroller tesis edilir ve bunlara ilişkin politika, prosedür ve süreçler yazılı hale getirilir, düzenli olarak gözden geçirilir, iş alanında gerçekleşen değişiklikler ve teknolojik gelişmeler doğrultusunda güncellenir, ilgili onay makamı tarafından onaylanır ve ilgililere duyurulur.
- Bilgi güvenliğine ilişkin yasal, düzenleyici, sözleşmesel ve diğer uygulanabilir gerekliliklere uyulur. Bilgi sistemleri aracılığıyla edinilen veya saklanan kişisel verilerin korunmasına yönelik gerekli kontroller tesis edilir ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ilgili diğer mevzuattan doğan yükümlülükler yerine getirilir.
- Şirket'in sahip olduğu bilgi varlıkları belirlenir, bunlara ilişkin envanter oluşturulur ve envanterin güncelliği korunur. Kullanımdan kaldırılan bilgi varlıklarına güvenli silme veya imha işlemleri uygulanır ve bu işlemler kayıl altına alınır; kullanımdan kaldırılan yazılım ve uygulamalara erişimler engellenir ve gerektiğinde bunlar arşivlenerek sistemden silinir.
- Kritik bilgi sistemlerinin bulunduğu veri merkezleri ve güvenli alanlar; yetkisiz fiziksel erişimlere, değişen ortam koşullarına, altyapı hizmeti kesintilerine ve olağanüstü sayılabilecek hallere karşı korunur. Destekleyici altyapının bakımı yılda en az bir defa gerçekleştirilir ve bu alanlara erişecek dış hizmet sağlayıcıların personellerine gizlilik sözleşmesi imzalatılarak ilgili personele refakat edilmesi sağlanır.
- Kurumsal ağın ve bilgi sistemlerinin güvenliğinde çok faktörlü kimlik doğrulama, erişim için yetkilendirme ve onay mekanizması olmak üzere çok katmanlı güvenlik yaklaşımı esas alınır. Uzaktan erişim yetkilendirmelerinde Bilgi Güvenliği Sorumlusu'nun onayı alınır ve uzaktan erişimlere ilişkin denetim izleri tutulur.
- Bilgi sistemlerine yönelik kapasite planlaması yapılır ve mevcut kapasite kullanımı izlenerek gelecekteki kapasite ihtiyaçları değerlendirilir; bilgi sistemlerinin performans ve yeterliliğinin korunması için gerekli önlemler alınır.
- Bilgi güvenliği ihlallerinin ve bilgi sistemlerine ilişkin güvenlik açıklarının yönetilmesine yönelik kontroller tesis edilir. Gerçekleşen ihlaller ve tespit edilen güvenlik açıkları mümkün olan en kısa sürede kayıt alına alınır, değerlendirilir ve gerekli işlemler gerçekleştirilir. Mevzuatta öngörülen durumlarda ilgili merciler ve ilgili kişiler derhal bilgilendirilir.
- Bilgi güvenliği ihlal olayları sonrasında, olayın etkileri, kök sebebi, olaya müdahale kapsamında gerçekleştirilen işlemler, görev alan kişiler ile harcanan zaman, maliyet ve iş gücünü kapsayan siber olay müdahale raporu hazırlanır ve üst yönetime sunulur. Kritik sistemlerin veya hassas verilerin etkilendiği ve uygulanabilir mevzuat uyarında bildirim yükümlülüğü doğduğu durumlarda rapor, ilgili kurum ve kişilere mevzuatta öngörülen süre içinde iletilir.
- Bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması tesis edilir. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağan dışı durumlar üst yönetime raporlanır. Denetim izleri yeterli güvenlik düzeyine sahip ortamlarda, yedekleri alınarak ve erişilebilirlikleri korunarak en az beş yıl süreyle saklanır.
- Şirket tarafından elektronik ortamda sunulan hizmetlerden yararlanan müşteriler, sunulan hizmetlerin şartları, riskleri ve istisnai durumları ile bu risklerden korunmak için kullanılabilecek yöntemler hakkında açıkça bilgilendirilir ve bilgilendirmenin yapıldığı ispatlanabilir şekilde kayıt altına alınır. Müşterilerin sorun ve şikayetlerini iletebilecekleri ve takip edebilecekleri mekanizmalar oluşturularak bu mekanizmalar aracılığıyla iletilen şikayet ve uyarılar değerlendirilerek tespit edilen aksaklıkların giderilmesi sağlanır.
- Kritik iş süreçlerini ve faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planı hazırlanır. İşbu plan, iş süreçlerini veya

bilgi sistemlerini etkileyen önemli değişikliklerden sonra ve her halükarda yılda en az bir defa gözden geçirilerek güncellenir.

- Bilgi sistemleri süreklilik planının etkinliğini ve güncelliğini değerlendirmek üzere yılda en az bir defa test gerçekleştirilir ve *(varsa)* ilgili dış hizmet sağlayıcılar da testlere dahil edilir. İşbu testlerin sonuçları üst yönetime raporlanır.
- Bilgi sistemleri, iş sürekliliği planında belirlenen önceliklere uygun olarak yedeklenir, yedeklerin en az bir kopyası farklı bir coğrafi konumda saklanır ve güvenliğine ilişkin gerekli önemler alınır. Kritik sistemlerin yedekten geri dönme testleri yılda en az bir defa gerçekleştirilir. Testin tarihi, kapsamı katılımcıları ve sonuçları kayıt altına alınarak yedeklerin ilgili saklama süreleri boyunca geri döndürülebilir olması sağlanır.
- Şirket bakımından ilgili mevzuat uyarınca zorunlu olduğu hallerde birincil ve ikincil sistemler yurt içinde bulundurulur ve ikincil sistemin, doğal ve çevresel felaketler bakımından birincil sistemle aynı risklere maruz kalmayacak bir konumda bulunması sağlanır.
- Bilgi güvenliği farkındalığının artırılması amacıyla personele, görev ve sorumluluklarına uygun olarak bilgi güvenliği gereksinimleri, riskler ve güncel tehditler hakkında yılda en az bir defa eğitim verilir.
- İşbu politika ve politikaya bağlı prosedür, talimat ve diğer alt düzenlemeler yılda en az bir defa ve ayrıca iş ihtiyaçlarında, bilgi sistemlerinde, siber tehditlerde, risklerde veya ilgili mevzuatta önemli değişiklik meydana gelmesi halinde gözden geçirilir ve gereklilik halinde güncellenir.
- Bilgi güvenliği yönetim sisteminin etkinliği düzenli olarak izlenir, gözden geçirilir ve sürekli olarak geliştirilir.

ÜST YÖNETİM

İşbu politikada geçen "**Üst Yönetim**" ifadesi; Yönetim Kurulu tarafından bilgi güvenliği ve bilgi sistemleri yönetimine ilişkin olarak yetkilendirilen kişi ya da grubu, ifade eder.

Şirket Yönetim Kurulu tarafından **Bilgi İşlem Müdürü**, işbu politika kapsamında üst yönetim olarak belirlenmiştir. Bu nedenle işbu politika kapsamında üst yönetime verilen görev ve yetkiler, Bilgi İşlem Müdürü tarafından yerine getirilir. Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi, izlenmesi, gözden geçirilmesi ve sürekli iyileştirilmesine ilişkin sorumluluk Üst Yönetim sıfatıyla Bilgi İşlem Müdürü'ne aittir.

Bilgi sistemleri güvenliğine ilişkin kontrollerin yerine getirilmesinden ve takibinden sorumlu olacak **Bilgi Güvenliği Sorumlusu;** bilgi sistemleri iç kontrolü, bilgi sistemleri denetimi, bilgi sistemleri yönetişimi ve kontrollerinin tesisi veya bilgi güvenliği alanlarından en az birinde yeterli teknik bilgiye sahip ve en az beş yıllık tecrübeye sahip, bilgi sistemleri yönetimine ilişkin gerekliliklerin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve görev bağımsızlığına sahip bir kişi olarak belirlenir. Bilgi Güvenliği Sorumlusu; bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetimi hakkında doğrudan üst yönetim sıfatıyla Bilgi İşlem Müdürü'ne raporlama yapar.

Üst yönetim sıfatıyla Bilgi İşlem Müdürü aşağıdaki görev ve sorumlulukları yerine getirir:

- İşbu Bilgi Güvenliği Politikası'nı hazırlamak, politikanın yılda en az bir defa ve ayrıca iş ihtiyaçları ile tehdit ve risklerde önemli değişiklik meydana gelmesi halinde gözden geçirilmesini ve gerektiğinde güncellenmesini sağlamak, politikayı ve politikada yapılacak değişiklikleri Yönetim Kurulu'nun onayına sunmak ve onaylanan politikanın personele ve ilgili diğer taraflara duyurulmasını sağlamak;

- Bilgi sistemlerinin yönetimine ilişkin kontrollerin tesis edilmesini, bunlara ilişkin politika, prosedür ve süreçlerin yazılı hale getirilmesini, düzenli olarak gözden geçirilerek güncellenmesini, ilgili onay makamı tarafından onaylanmasını ve ilgililere duyurulmasını sağlamak;
- İşbu politikanın ve bilgi sistemleri stratejisinin uygulanmasını gözetmek, bilgi sistemleri stratejisinin Şirket'in iş hedefleriyle uyumunu izlemek ve gerektiğinde iyileştirici faaliyetlerin gerçekleştirilmesini sağlamak;
- Bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin, sorumlulukların ve görev tanımlarının belirlenmesi ve yazılı hale getirilmesi ile görevlendirmelerin görevler ayrılığı ilkesi çerçevesinde yapılmasını sağlamak;
- Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeleri gözden geçirmek ve ilgili risklerin yönetilebilirliğini dikkate alarak onaylamak; projelerde görev alan personelin uzmanlığının projenin teknik gereksinimlerini karşılayabilecek nitelikte olmasını sağlamak;
- Bilgi güvenliği önlemlerinin uygun düzeye getirilmesi ve bu amaçla yürütülecek faaliyetler için gerekli insan kaynağı, teknoloji, finansal kaynak ve organizasyonel desteğin sağlanmasını temin etmek;
- Bilgi güvenliği politikalarının ve bilgi güvenliğine ilişkin sorumlulukların yılda en az bir defa gözden geçirilmesini ve ilgili onay makamının onayına sunulmasını; bilgi güvenliği ihlallerinin takip edilmesini ve yılda en az bir defa değerlendirilmesini ve personele gerekli bilgi güvenliği eğitimlerinin verilmesini sağlamak;
- Bilgi sistemlerine ilişkin risklerin belirlenmesi, ölçülmesi, izlenmesi, işlenmesi ve raporlanmasına yönelik risk yönetimi süreç ve prosedürlerinin tesis edilmesini ve güncel tutulmasını sağlamak; risk kabul kriterleri ile risk işleme seçeneklerini, risk analizini ve iyileştirici faaliyetleri değerlendirmek ve onaylamak;
- Bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetilmesi, bilgi varlıklarının gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması ve bilgi sistemlerinin etkin şekilde işletilmesi amacıyla gerekli süreç ve kontrollerin geliştirilmesini sağlamak;
- Bilgi sistemleri süreçleri ve kontrollerine ilişkin etkinlik, yeterlilik ve mevzuata uyum değerlendirmeleri sonucunda tespit edilen önemli kontrol eksiklikleri ve yapılan çalışmalar hakkında kendisine sunulan raporları değerlendirmek ve gerekli önlemlerin alınmasını sağlamak;
- Bilgi Güvenliği Sorumlusu'nun işbu politikada öngörülen teknik bilgi, tecrübe ve görev bağımsızlığı şartlarını taşımasını ve doğrudan kendisine bağlı çalışmasını sağlamak; Bilgi Güvenliği Sorumlusu tarafından kendisine sunulan raporları değerlendirmek;
- Bilgi varlıklarının güvenlik sınıfının belirlenmesine ilişkin kılavuzu ve bilgi varlıklarının uygun kullanımına ilişkin prosedürleri onaylamak;
- Bilgi güvenliği ihlal olaylarına müdahale planını onaylamak, kendisine sunulan siber olaylara müdahale raporlarını değerlendirmek ve kritik sistemlerin veya hassas verilerin etkilendiği durumlarda raporların uygulanabilir mevzuat uyarınca ilgili kurum ve ilgili kişilere iletilmesini sağlamak;
- Bilgi sistemleri süreklilik planını ve yedekleme çizelgesini onaylamak, bilgi sistemleri süreklilik planına ilişkin test sonuçlarını ve denetim izlerinin bütünlüğü hakkında raporlanan olağan dışı durumları değerlendirmek ve gerekli önlemlerin alınmasını sağlamak;
- İşbu politikanın "Dışarıdan Hizmet Alımı" başlıklı bölümünde üst yönetime verilen görev ve sorumlulukları yerine getirmek.

YÖNETİM KURULU

Yönetim Kurulu aşağıdaki görev ve sorumlulukları yerine getirir:

- İşbu politika kapsamında üst yönetim olarak görev alacak kişi veya grubu belirlemek, bu kapsamda görev ve yetkilerinin değiştirilmesine veya görevlendirmenin sona erdirilmesine karar vermek;
- Üst yönetim tarafından hazırlanan Bilgi İşlem Politikası'nı ve işbu politikada yapılacak değişiklikleri değerlendirmek ve onaylamak;
- İşbu politika kapsamında bilgi sistemlerinin kontrollerinin etkin, yeterli ve mevzuata uyumlu şekilde tesis edilmesini, değerlendirilmesini ve gözetimini sağlamak;
- Yönetim Kurulunun onayına tabi tutulan diğer bilgi sistemleri politika ve üst düzey düzenlemelerini değerlendirmek ve onaylamak;
- Üst yönetim tarafından kendisine sunulan önemli bilgi güvenliği risklerini, kontrol eksikliklerini ve iyileştirici faaliyetleri değerlendirmek; gerekli tedbirlerin alınmasına karar vermek ve alınan kararların uygulanmasını gözetmek.

Üst yönetimin veya Bilgi Güvenliği Sorumlusu'nun belirlenmesi ya da bilgi sistemleri kapsamında dışarıdan hizmet alınması, Yönetim Kurulu'nun bilgi sistemleri kontrollerinin etkin, yeterli ve mevzuata uyumlu şekilde tesis edilmesi, değerlendirilmesi ve gözetimine ilişkin sorumluluğunu ortadan kaldırmaz.

DIŞARIDAN HİZMET ALIMI

Bilgi sistemleri kapsamında dışarıdan hizmet alınması, Şirket'in ilgili mevzuattan ve işbu politikadan doğan yükümlülüklerini, nihai sorumluluğunu veya karar alma yetkisini dış hizmet sağlayıcıya devrettiği şeklinde yorumlanamaz. Dışarıdan alınan hizmetlerde ölçme, değerlendirme, raporlama, güvenlik ve yetkilendirme süreçlerine ilişkin nihai sorumluluk ve karar alma yetkisi Şirket'te kalır.

Üst Yönetim tarafından, bilgi sistemleri kapsamında dışarıdan hizmet alımının doğuracağı risklerin yeterli düzeyde değerlendirilmesine ve yönetilmesine ve dış hizmet sağlayıcılarla ilişkilerin etkin şekilde yürütülmesine imkan sağlayacak bir gözetim mekanizması tesis edilir. Bu mekanizma kapsamında asgari olarak aşağıdaki hususlar gözetilir:

- Dışarıdan alınan bilgi sistemleri hizmeti kapsamındaki bütün sistem ve süreçlerin Şirket'in risk yönetimi, bilgi güvenliği ve müşteri mahremiyeti ilkelerine uygun olması;
- Şirket verilerinin dış hizmet sağlayıcıya aktarılmasının gerekli olduğu durumlarda, dış hizmet sağlayıcının bilgi güvenliğine ilişkin ilke ve uygulamalarının en az Şirket tarafından uygulanan düzeyde olması;
- Dışarıdan alınan hizmete ilişkin koşulların Şirket'in iş sürekliliği dikkate alınarak düzenlenmesi ve bu kapsamda gerekli önlemlerin alınması;
- Dışarıdan alınan hizmetin Şirket'in yasal yükümlülüklerini yerine getirmesini veya etkin şekilde denetlenmesini engelleyici nitelikte olmaması;
- Dış hizmet sağlayıcıya karar verilmeden önce, dış hizmet sağlayıcının hizmeti istenilen kalitede gerçekleştirebilmesi için gerekli teknik donanım ve altyapıya, mali güce, tecrübeye, bilgi birikimine ve insan kaynağına sahip olup olmadığının değerlendirilmesi; yoğunlaşma riskinin, hizmetten çıkış stratejisinin ve hizmetin ikame edilebilirliğinin dikkate alınması ve bu değerlendirmeler sonucunda hazırlanan teknik yeterlilik raporunun Üst Yönetimin onayına sunulması;
- Dışarıdan alınan hizmetin kapsamının, dış hizmet sağlayıcının iletişim bilgilerinin, hizmetin geçerlilik süresinin, hizmet seviyesinin ve kritiklik durumunun yazılı hale getirilmesi.

Üst Yönetim; dışarıdan alınan kritik hizmetlerin erişilebilirliğini, performansını ve kalitesini, bu hizmetler kapsamında gerçekleşen güvenlik ihlallerini ve dış hizmet sağlayıcının güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu takip etmek üzere yeterli bilgi ve tecrübeye sahip sorumlular belirler. Belirlenen sorumlular tarafından söz konusu hususları kapsayan bir değerlendirme raporu yılda en az bir defa hazırlanarak Üst Yönetime sunulur.

Dışarıdan hizmet alımına ilişkin koşullar, hizmetin kapsamı ve ilgili diğer bütün hususlar, dış hizmet sağlayıcının da taraf olduğu yazılı bir sözleşmeyle düzenlenir. Sözleşmede asgari olarak aşağıdaki hususlara yer verilir:

- Hizmet seviyelerine ilişkin tanımlamalar;
- Hizmetin sona erdirilmesine ilişkin koşullar ile hizmetin sona ermesi halinde Şirket'e ait bütün verilerin Şirket'e teslim edilmesine ve dış hizmet sağlayıcı nezdinde bulunan kopyalarının güvenli ve geri döndürülemez şekilde imha edilmesine ilişkin yükümlülükler;
- Hizmetin beklenmedik şekilde sona ermesi veya kesintiye uğraması halinde uygulanacak yaptırımlar;
- Şirket'in bilgi güvenliği politikası kapsamında önem taşıyan hususlara ilişkin gereklilikler ile dış hizmet sağlayıcının hizmet süresince ve hizmetin sona ermesinden sonra Şirket hakkında edindiği bilgileri gizli tutmasına ilişkin yükümlülükler;
- Sözleşme kapsamında bir ürün üretilmesinin öngörülmesi halinde, ürünün sahipliği ile fikri ve sınai mülkiyet haklarını düzenleyen hükümler;
- Dış hizmet sağlayıcı bakımından yükümlülük oluşturan sözleşme hükümlerinin, hizmetin ifasında görev alacak alt yükleniciler bakımından da bağlayıcı olmasını sağlayacak hükümler;
- Dış hizmet sağlayıcının, Şirket veya uygulanabilir mevzuat uyarınca yetkili kurum ve kuruluşlar tarafından talep edilen bilgi ve belgeleri istenilen zamanda ve nitelikte sağlama yükümlülüğü ile söz konusu yetkili kurum ve kuruluşların hizmetle ilgili olarak dış hizmet sağlayıcı nezdindeki bilgi, belge ve kayıtlara mevzuattan doğan erişim haklarının kullanılmasını sağlayacak hükümler;
- Dış hizmet sağlayıcı nezdinde gerçekleşen güvenlik ihlali, veri sızıntısı veya benzeri olayların derhal Şirket'e bildirilmesine ilişkin yükümlülükler;
- Şirket'in dış hizmet sağlayıcının sözleşme kapsamındaki faaliyetlerini izlemesine ve değerlendirmesine ilişkin esaslar;
- Dışarıdan hizmet alımına konu faaliyet bakımından ilgili mevzuatla Şirket'e getirilen yükümlülüklerin dış hizmet sağlayıcı tarafından da yerine getirilmesini sağlayacak hükümler.

Kritik olmayan hizmetlerin, yukarıda belirtilen hususların sözleşmeye dahil edilmesinin mümkün olmaması nedeniyle standart sözleşmelerle alınması halinde, standart sözleşme kullanılmasının gerekçesi yazılı hale getirilir.

Dış hizmet sağlayıcılara tanınacak fiziksel veya mantıksal erişim hakları özel olarak değerlendirilir. Bu erişimler için risk değerlendirmesi yapılır ve gerektiğinde ek kontroller tesis edilir. Risk değerlendirmesinde ihtiyaç duyulan erişim türü, erişilecek verinin hassasiyeti ve erişimin bilgi güvenliği üzerindeki etkileri dikkate alınır. Erişim hakları işin gerektirdiği en düşük yetkiyle sınırlandırılır ve gerektiğinde belirli bir süreyle tanımlanır. Hizmetin sona ermesi üzerine dış hizmet sağlayıcıya ve personeline tanınan bütün erişim hakları iptal edilir.

Dışarıdan alınan hizmetler kapsamında gerçekleştirilen işlemlere ilişkin denetim izlerinin tutulması ve bu denetim izlerine Şirket tarafından erişilebilmesi sağlanır. Dış hizmet sağlayıcılarla gerçekleştirilen veri

aktarımlarında, verilerin kötüye kullanılmasını, kaybolmasını, yetkisiz şekilde değiştirilmesini veya bozulmasını önleyecek güvenlik önlemleri alınır ve kişisel veri aktarımlarında 6698 sayılı Kişisel Verilerin Korunması Kanunu ile ilgili diğer mevzuata uyulur.

Şirket, faaliyetlerinin tamamı veya bir bölümü için bulut hizmeti kullanabilir. Bulut hizmetlerinin alınması, kullanılması ve yönetilmesi dışarıdan hizmet alımı sayılır. Bulut hizmeti kullanımında Şirket'in tabi olduğu mevzuat ile işbu politikanın bilgi sistemleri sürekliliğine ve dışarıdan hizmet alımına ilişkin hükümleri ile dikkate alınır.

Dışarıdan temin edilen yazılım, donanım, işletim sistemi veya bunların bir veya birkaçını içeren cihaz ve sistemlerin, mevcut güvenlik önlemlerini aşarak erişim sağlamak amacıyla özel olarak tasarlanmış veya kasıtlı olarak dahil edilmiş boşluklar veya güvenlik açıkları barındırmadığına ilişkin taahhütname dağıtıcıdan, tedarikçiden veya üreticiden alınır.

Bilgi Güvenliği Sorumlusu, dışarıdan hizmet alımı yoluyla veya grup şirketleri arasında imzalanacak hizmet sözleşmeleri kapsamında belirlenebilir; bilgi güvenliği sorumluluğuna ilişkin görevler ortak istihdam veya yarı zamanlı çalışma modeliyle yerine getirilebilir. Bu hallerde Bilgi Güvenliği Sorumlusunun Tebliğ'de aranan nitelikleri ve görev bağımsızlığını taşıması, doğrudan Üst Yönetime bağlı çalışması ve bu bölümde düzenlenen dışarıdan hizmet alımı koşullarına uyulması zorunludur.

YÜRÜRLÜK VE SAİR HUSUSLAR

Bu politikaya ve politikayı destekleyen alt politika, prosedür ve talimatlara uyum; şirket çalışanları ve yöneticileri ile bu yükümlülüğün kendilerine uygulanacağı sözleşme, taahhütname veya sair bağlayıcı düzenlemelerde öngörülen ölçüde danışmanların, tedarikçilerin ve diğer ilgili tarafların yükümlülüğündedir.

Politika hükümlerine aykırı davranışlar, ilgilisine göre iş sözleşmeleri, Şirket iç düzenlemeleri, ilgili taraflarla akdedilen sözleşmeler ve uygulanabilir mevzuat çerçevesinde işleme konu edilir. Hukuki, idari ve cezai sorumluluk, ilgili mevzuat ve somut olayın özelliklerine göre belirlenir.

Bu politika Yönetim Kurulu onayını müteakip yayımlandığı tarihte yürürlüğe girer ve Bilgi İşlem Müdürü tarafından yürütülür.