1. Amaç

Şirket; bilgi güvenliğini yöneterek, iş süreçlerinin bilgi güvenliği riskleri karşısında en az etkiyle işlemesini güvence altına almayı hedeflemektedir. Bu politika ile bilgi sistemlerindeki süreçlerde üretilen, kullanılan ve saklanan bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol yapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarının gözetim altında tutulması amaçlanmaktadır.

2. Kapsam

Politika, Şirket bünyesindeki bilgi güvenliği faaliyetlerini kapsar.

3. Tanımlar

Varlık: Şirket için değer ifade eden her şeydir.

Bilgi: Şirketin faaliyetlerini sürdürmesi için kullanılan veya kullanılmış her türlü fiziksel ve elektronik veri ile bu verilerin yorumlanması ile elde edilen türevleridir.

Bilgi Güvenliği: Bilginin bütünlüğünün, kullanılabilirliğinin ve gizliliğinin sağlanması sürecidir.

Bilgi Güvenliği Olayı: İş faaliyetlerini riske atma ve bilgi güvenliğini tehlikeye düşürme olasılığı yüksek olan tek başına veya bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olaylarıdır.

Bütünlük: Bilgilerin herhangi bir kaza ya da yasa dışı işlemle değiştirilmediğinin garantisidir. Veri tutarlı, tam ve doğru olmalıdır.

Gizlilik: Bilgiye, politikalarda belirlenen şartlar ve kurallar ile sadece yetki verilen kişilerce erişildiğinin garantisidir.

Kullanılabilirlik: İhtiyaç olduğu anda bilgiye ulaşabilme ve kullanabilme garantisidir.

Kontrol: Riskin politikalar, prosedürler, rehberler, teknolojik çözümler, organizasyonel yapılar ile gerektiğinde bir defaya mahsus alınan önlemler yoluyla yönetilmesini sağlayan ve idari, teknik, yönetimsel veya yasal olabilen araçlardır.

4. Görev ve Sorumluluklar

Yönetim Kurulu

Şirket bünyesinde bilgi güvenliğinin sağlanmasında nihai sorumluluk Yönetim Kurulu'na aittir. Yönetim Kurulu, bilgi sistemlerine ilişkin güvenlik önlemlerinin yeterli düzeye getirilmesi noktasında gerekli kararlılığı göstererek, bu amaç doğrultusunda yeterli kaynağın sağlanmasından sorumludur. Yine bu amaç doğrultusunda Yönetim Kurulu, Şirket genelini kapsayan bir bilgi güvenliği yönetim sistemi tesis eder.

Yönetim Kurulu ayrıca, şirket varlıklarının korunması ve bilgi güvenliğinin sağlanmasına yönelik olarak sağlam ve güncel bir plan oluşturulmasını ve bilgi güvenliği risklerinin uygun şekilde yönetilmesi amacıyla etkin bir yönetişim sağlanmasını temin eder.

Üst Yönetim

Genel Müdür/Yönetim Kurulu Başkanı, Bilgi Güvenliği Komitesine başkanlık eder. Şirket bünyesinde bilgi sistemleri güvenlik fonksiyonları doğrudan Genel Müdür/Yönetim Kurulu Başkanı' na bağlı olup, yıllık bilgi güvenliği planının uygulanması Genel Müdür/Yönetim Kurulu Başkanı, güvencesi ile sağlanır.

Bilgi Güvenliği Komitesi

Şirket genelinde bilgi güvenliği politikasının oluşturulması ve ilgili politikanın uygulanması faaliyetlerinin yürütülmesi amacıyla Bilgi Güvenliği Komitesi oluşturulur. Bilgi Güvenliği Komitesi düzenli aralıklarla yılda en az bir defa toplanır.

Bilgi Güvenliği Komitesi'nin sorumlulukları aşağıda listelenmiştir.

- Şirket bilgi varlıklarına ilişkin güvenlik gereksinimlerinin tespit edilmesi, uygulanması ve izlenmesi,
- Bilgi güvenliği bilincinin oluşturması ve farkındalık seviyesinin artırılmasına yönelik çalışmaların yönetilmesi,
- Şirket genelinde bilgi güvenliğinin sağlanmasına yönelik gerekli Bölümlerin desteğinin alınması ve Bölümler arası koordinasyonunun sağlanması,
- Bilgi güvenliği ile ilişkili tüm üst düzey kararların alınması,
- Bilgi güvenliğinin sağlanması ve kabul edilebilir risk seviyelerinin belirlenmesi,
- Şirket bilgi güvenliği ve gizliliği ile ilgili politika, prosedür ve ilgili belgelerin gözetilmesi,
- Bilgi güvenliğine ilişkin olarak oluşturulan politika ve prosedürlerin uygulanması sırasında ortaya çıkan ve bilgi sistemleri güvenlik fonksiyonu tarafından iletilen istisnai durumların değerlendirmesi,
- Yıllık Bilgi Güvenliği Planının onaylanması,
- Bilgi güvenliğinin iş ihtiyaçları stratejilerine uygun olmasına ve Şirket kültüründe kabul görmesine önderlik edilmesi,
- Bilgi Güvenliği Politikası hükümlerinin Şirket varlıkları için uygulanması ve bilgi güvenliği ile ilgili tüm çalışmalar için net bir yön ve yönetim desteği sağlanması,
- Yılda en az bir defa yönetim kuruluna raporlama yapılması.

Bilgi Güvenliği Komitesinin koordinasyonu Bilgi Güvenliği Sorumlusu tarafından yerine getirilir. Komite; Üst Yönetim, Bölüm Yöneticileri, Bilgi Teknolojileri Sorumlusu, Bilgi Güvenliği Sorumlusu, İnsan Kaynakları Sorumlusu, Hukuk birimi ile katılımı gerekli görülen Bölüm çalışanlarından oluşur. Bilgi Güvenliği Komitesi toplantılarında alınan kararlar Bilgi Güvenliği Sorumlusu aracılığıyla tüm Şirkete duyurulur.

Bilgi Teknolojileri Sorumlusu

- Bilgi sistemlerinin geliştirilmesi, yönetimi, işletimi için kullanılan teknolojilerin Şirkete uyarlanmasından,
- BT süreçlerinin düzenlenmesinden ve sağlıklı işleyişi için gerekli kontrollerin tesisinde kritik bilgilerin gizlilik, bütünlük ve erişilebilirliğinin sağlandığının gözetiminden,
- Bilgi Teknolojileri alanı kapsamında iş ihtiyaçlarını karşılarken, Yönetim Kurulu tarafından onaylanmış Bilgi Güvenliği Politikasına ve yayınlanmış prosedürlere göre yürütüldüğünün gözetiminden,
- Bilgi Güvenliği Politikasına ve ilgili prosedürlere uygun şekilde bilgi teknolojileri süreçleri ile altyapısını tasarlamak ve yapılandırmaktan, sorumlusu olduğu bilgi varlıklarında ve iş süreçlerinde politika ve prosedürlerde yazan kuralların uygulanmasından sorumludur.

Bilgi Güvenliği Sorumlusu

- Bilgi sistemleri güvenliğine ilişkin kontrol gereksinimlerinin belirlenmesine katkı sağlar, bu gereksinimlerin ilgili birimlerce yerine getirilme durumunu izler ve tespitlerini üst yönetime raporlar.
- Bilgi güvenliği risklerinin belirlenmesi, değerlendirilmesi, kayıt altına alınması ve takibine yönelik süreçleri koordine eder.
- Bilgi güvenliği stratejisi, politika ve prosedür taslaklarının ilgili birimlerle koordineli olarak hazırlanmasına katkı sağlar ve üst yönetimin değerlendirmesine sunar.
- Bilgi güvenliğini etkileyebilecek değişiklik ve projelere ilişkin güvenlik değerlendirmesi yapar ve görüşünü ilgili karar mercilerine bildirir.
- Siber güvenlik olaylarının kayıt altına alınması, sınıflandırılması, değerlendirilmesi, ilgili taraflara iletilmesi ve müdahale aksiyonlarının takibini koordine eder.
- Bilgi güvenliği bulguları ile mevzuat uyumuna ilişkin eksiklikleri takip eder ve üst yönetime raporlar.
- Bilgi güvenliği farkındalık ihtiyaçlarının ve eğitim içeriklerinin belirlenmesine katkı sağlar ve eğitimlerin gerçekleştirilme durumunu izler.
- Bilgi güvenliği faaliyetleri, riskler, ihlaller ve aksiyonların durumu hakkında periyodik olarak üst yönetime ve yılda en az bir kez Yönetim Kuruluna raporlama yapar.

Tüm Çalışanlar

Bilgi Güvenliği Politikası ve prosedürlerine uyum sağlayarak, bu doğrultuda hareket etmekten, bilgi güvenliği farkındalık eğitimlerine katılım sağlamaktan, karşılaşılan güvenlik ihlal olaylarını Bilgi Güvenliği Birimi'ne bildirmekten sorumludur.

Dış Hizmet Çalışanları

Tüm dış hizmet çalışanları, Şirket Bilgi Güvenliği Politikası ve kendi işleyişlerine ilişkin güvenlik prosedürlerine uyum sağlamaktan sorumludur.

5. İçerik ve Uygulama

5.1. Bilgi Güvenliği Yönetimine İlişkin Temel İlkeler

- Bilgi sistemlerinin yapısının, Şirketin ölçeği, faaliyetlerin ve sunulan ürünlerin niteliği, çeşitliliği ve stratejik hedefleri ile uyumlu olması; bilgi sistemleri ile içerdiği verinin güvenilir, doğru, eksiksiz, izlenebilir, tutarlı, erişilebilir ve ihtiyaçları karşılayacak nitelikte oluşturulması esastır. Bilgi sistemleri asgari olarak,
    - Şirket ile ilgili tüm bilgilerin yurt içinde elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasını veya yedeklenmesini ve kullanılmasını sağlar.
    - Şirket, dışarıdan gelecek bir siber saldırıya karşı gerekli önlemleri alır ve her yıl sızma testi yaptırır.
    - Dış ağlardan gelebilecek tehditler için ağ kontrol güvenlik sistemleri tesis edilir.

- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere iş sürekliliği planı oluşturulur ve doğal afetler/teknik problemler kaynaklı kesinti ve risklere karşı iş süreçlerinin korunması sağlanır.

- Bilgi sistemleri ile içerdiği verinin güvenli biçimde saklanması esastır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilir ve buna göre yedeklenir.
- Bilgi güvenliğinin temininde ve Şirket bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılır.
- Bilgi sistemlerinin kullanımında; görev ve sorumluluklar göz önünde bulundurularak, gerekli olan en kısıtlı yetki ve erişim hakkının verilmesi sağlanır.
- Bilgi sistemlerinin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulması sağlanır.
- Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir.
- Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ile Şirket bilgilerinin gizliliğini sağlamak esastır.
- Bilgi sistemleri kullanılarak gerçekleştirilen; müşterilere ve Şirket faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri oluşturulur. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınır.
- Bilgi sistemlerinin bulunduğu alanın güvenliği sağlanır, alanın içeriden ve dışarıdan gelebilecek tehditlere karşı korunması için gerekli tedbirler alınır.
- Uygulamaya konulan bilgi sistemlerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni eklenecek bilgi sistemlerine ait envanterin, Şirket risk profili üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri işleyişi yenilenir.
- Şirket bilgi güvenliğini ve iş fonksiyonlarını yerine getirmek için üçüncü taraflardan dış hizmet alımı yapabilir.
- Dış hizmet alınması durumunda üçüncü tarafların çalışanlarının Şirket bilgi varlıklarına erişim konusunda Bilgi Güvenliği Politikası hükümlerine uyumu, dış hizmet alımına konu sözleşme ile güvence altına alınır.

5.2. Bilgi Güvenliği Politikası Uygulamaları

5.2.1. Bilgi Sistemleri Varlıklarının Yönetimi

Basılı ve dijital ortamda oluşturulan, iletilen, saklanan veya sözlü olarak paylaşılan Şirket' e ait tüm veriler Şirket bilgi varlığı olarak kabul edilir. Verinin iletilmesinde, işlenmesinde, erişilmesinde, saklanmasında, imhasında kullanılan uygulama, yazılım ve donanımlar da bilgi varlıkları kapsamına girer.

Şirket, bilgi varlıklarının ve bu veriyle ilgili tüm varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini sağlayarak kazara veya kasti biçimde hasar görmesini, değişmesini, ifşa olmasını veya kaybolmasını önler. Bunun için bilgi sistemleri varlık envanterini oluşturur, varlık değerlendirmesi yapar ve sınıflandırır. Şirket; bilgilerin bu sınıflandırmaya uygun olarak kullanılmasını sağlar.

Şirket, bilgi sistemleri varlık envanterini güncel olarak takip eder ve envanter kayıtlarını saklar. Envanterden çıkarılan donanımların şirkete ait bilgi taşımaması için gerekli tedbirler alır.

Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak bilgi sistemleri varlık yönetimi süreci ***Varlık Yönetimi Prosedürü*** dokümanında detaylandırılmıştır.

5.2.2. Risklerin Değerlendirilmesi

Şirket bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenliği Sorumlusu tarafından belirlenir ve tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile Şirket bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıkları ile ilgili oluşabilecek risklerin tanımlanması, seviyelerinin belirlenmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir. Bilgi Güvenliği risklerini de içeren bilgi teknolojileri faaliyetleri sırasında kullanılan risk değerlendirme yaklaşımı ve yönetimi ***Bilgi Sistemleri Risk Yönetimi Prosedürü*** dokümanında detaylandırılmıştır.

5.2.3. Bilgi Güvenliği Farkındalığının Yaratılması

Şirket; bütün personeli için farkındalık eğitim gerekliliklerini belirler ve personeline uygun bir şekilde eğitim sağlar. İşe yeni alınan her çalışan için oryantasyon ve bilgi güvenliği konusunda zorunlu olarak eğitim ataması yapılır. Bilgi güvenliği eğitimleri her yıl düzenli olacak şekilde tekrarlanır. Şirket kendi çalışanlarına ve danışmanlarına bilgi güvenliği politikalarını okuduklarına ve uyacaklarına dair imzalı onaylarını alır.

5.2.4. Fiziksel ve Çevresel Güvenlik

Şirket, bilgi işleme faaliyetlerinin gerçekleştiği binalara, alanlara yetki dışı fiziksel erişimi, müdahale ve hasarı engellemek amacı ile fiziksel güvenlik önlemleri alır. Sistem odasına giriş/çıkışlar kontrol altına alınır ve kamera ile izlenir ve bu sayede bilgi varlıklarının kaybı, hasarı, çalınması, tehlikeye girmesi ve kuruluşun faaliyetinin kesintiye uğraması engellenir. Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak fiziksel ve çevresel güvenlik yaklaşımı ve yönetimi ***Fiziksel ve Çevresel Güvenlik Yönetimi Prosedürü*** dokümanında detaylandırılmıştır.

5.2.5. Yetkilendirme ve Erişim Kontrolü

Şirket, veri tabanlarına, uygulamalara ve sistemlere erişim için, görev ve sorumluluklar dahilinde uygun yetkilendirme ve erişim kontrolü tesis eder.

- Veri tabanlarına, uygulamalara ve sistemlere erişim için uygun bir yetkilendirme ve erişim kontrolü tesis edilir. Görev ve sorumluluklar göz önünde bulundurularak, gerekli olan en kısıtlı yetki ve erişim hakkının verilmesi esastır.
- Yetkiler ve erişim hakları yılda bir kez gözden geçirilir, yetkilerin en az yetki prensibine uyumu kontrol edilir.
- Sistem, servis ve veriye sadece gerekli yetkiye sahip kullanıcı, taraf ve sistemlerin erişimi sağlanır.
- Şirket, veri tabanlarına, uygulamalara ve sistemlere yapılan yetkisiz erişim teşebbüslerini kayıt altına alır ve gözden geçirir.
- Şirket, sunmakta olduğu hizmetlerin tasarımı, geliştirilmesi, test edilmesi ve sürdürülmesi aşamalarında, görevler ayrılığı prensibine uygun olarak geliştirme, test ve üretim ortamlarının birbirinden ayrı tutulmasını sağlar. Süreçler ve sistemler, kritik bir işlemin tek bir kişi tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkân vermeyecek şekilde tasarlanır ve işletilir.
- Şirket, geçici yetkilendirmeler için yetkilendirmenin yapılacağı şartları ve geçerli olacağı süreyi belirler. Geçici yetkilendirmeye ilişkin ilave iz kaydı tutulmasını sağlar.
- Şirket veya bünyesinde görev yapan dış hizmet çalışanlarının görevlerinin sonlanması durumunda ilgili tüm yetkilendirmelerin ivedilikle sonlandırılması sağlanır.

Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak Şirket uygulamalarının erişim ve yetkilendirme süreci ***Erişim Yetkilendirme ve Kontrol Prosedürü*** dokümanında detaylandırılmıştır.

5.2.6. Kimlik Doğrulama ve Şifre Kullanımı

Şirket, bilgi sistemleri üzerinde gerçekleşen işlemler için işlemlerin türünü, niteliğini, bir ihlal halinde oluşabilecek kayıpları, işlem çeşidini ve verinin hassasiyet derecesini dikkate alır ve buna uygun bir kimlik doğrulama mekanizması kurulmasını sağlar. Şirket, kimlik doğrulamada inkâr edilemezliği sağlar. Tüm kullanıcılara ait kimlik doğrulama bilgilerinin gizliliğine ve güvenliğine yönelik gerekli önlemleri alır.

Kimlik doğrulamada kullanılacak parolaların geçerlilik süresinin, karmaşıklığının ve uzunluğunun günün teknolojisine ve işlemin niteliğine uygun olması sağlanır. Dış hizmet sağlayıcılarında görevli personelin şirket sistemlerine uzaktan erişimi esnasında yapılacak kimlik doğrulama, en az şirket personeli ile aynı seviyede güvenlik sağlanarak yapılır. Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak Şirket uygulamalarının kimlik doğrulama süreci ***Kimlik Doğrulama ve Şifre Kullanımı Prosedürü*** dokümanında detaylandırılmıştır.

5.2.7. Değişiklik, Geliştirme ve Bakımı

Şirket sistem geliştirmeleri Bilgi Teknolojileri Bölümü tarafından planlanır ve izlenir. Tüm geliştirmeler, test edilir ve canlı ortama alınır. Üretim ortamında kullanılan yazılımların test ortamında test edilip onaylanan versiyon ile aynı olması sağlanır. Dış kaynak kullanılarak geliştirilen ve satın alınan yazılımların Şirket standartlarına paralel olarak geliştirme, test, doğrulama ve kurulum aşamalarında geçmesi sağlanır. Değişiklik yönetimi süreci ***Değişiklik Yönetimi Prosedürü*** dokümanında detaylandırılmıştır.

5.2.8. Bilgi Güvenliği İhlalleri Yönetimi

Kapsam içindeki süreçlere katılmak üzere yetkilendirilmiş tüm çalışanlar, kapsam dâhilindeki işleyişlere ilişkin fark ettikleri veya şüphelendikleri tüm güvenlik zafiyetlerini, risklerini ve vakalarını Bilgi Güvenliği Birimi'ne e-posta yolu ile iletir. Bilgi Güvenliği Birimi bildirilen vaka ile ilgili olarak vaka kaydı oluşturarak, inceleme sağlar.

Vakalar incelendikten sonra vakanın neden meydana geldiğinin mutlaka cevaplanması gereklidir. Vakanın oluşmasına neden olan eksiklikler ve muhtemel riskler detaylı şekilde incelendikten sonra ihtiyaç duyulan uygun kontrol konusunda vakadan etkilenen iş süreci veya bilgi varlıklarının iş ve teknik sahipleri bilgilendirilirler. Bu bilgilendirmeyi takiben iş ve teknik sahip uygun kontrolü devreye alır. Ayrıca Şirket'teki diğer bilgi varlıklarında da benzer risk yaşanmaması için vakaya ilişkin gerçekleştirilen düzeltici faaliyetin benzer durumdaki diğer varlıklarda da gerçekleştirilmesi için ilgili iş ve teknik sahipleri bilgilendirilir.

Vakalara ilişkin incelemeler yapılırken vakanın niteliğine göre vaka sorumlusu vakanın hukuksal boyutunun oluşacağını öngörerek vaka analizi sırasında Hukuk Müşavirliği desteği almayı tercih edebilir. Bu tür durumlarda delillerin hukuka uygun şekilde ele alınması sağlanır.

Bilgi güvenliği yönetimi faaliyetleri sırasında Şirket uygulamalarının ihlal olayı süreci ***Siber Olaylara Müdahale Süreci Prosedürü*** dokümanında detaylandırılmıştır.

5.2.9. Bilgi Sistemleri Süreklilik Planı

Şirket, faaliyetlerini destekleyen bilgi sistemleri servislerinin sürekliliğini sağlamak üzere bir bilgi sistemleri süreklilik planı hazırlar ve doğal afetler ve teknik problemler kaynaklı kesinti ve risklere karşın iş süreçlerinin korunması sağlar. Bilgi sistemleri süreklilik planı güncel tutulur, bilgi sistemleri sürekliliğini etkileyecek olay ya da değişikliklerden sonra veya her yıl gözden geçirilerek, güncellenir.

Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak Şirket uygulamalarının süreklilik planı süreci ***Bilgi Sistemleri İş Sürekliliği Prosedürü*** dokümanında detaylandırılmıştır.

5.2.10. Uyum

Tüm Şirket çalışanları, ilgili yasalar, yönetmelikler ve sözleşmelerden doğan güvenlik gereksinimlerine, fikri mülkiyet haklarına, lisans anlaşmalarına ve Şirket tarafından belirlenen güvenlik gereksinimlerine uymakla yükümlüdürler. Yöneticiler sorumluluk alanlarındaki tüm süreçlerin işletilmesinde güvenlik politikalarına ve standartlara uyumu temin eder. Tüm çalışanlar, Şirket verilerinin gizlilik derecelerine uygun şekilde kullanımı konusunda sorumludurlar.

Şirket'in bilgi güvenliği politikalarına uyumun denetlenmesi ve bilgi güvenliği gözden geçirme faaliyetleri Şirket'in Bilgi Güvenliği Sorumlusu tarafından gerçekleştirilir ve uyum durumu yılda en az bir defa Yönetim Kuruluna raporlanır.

5.2.11. Denetim İzi

Şirket, faaliyetlerine ilişkin etkin bir denetim izi mekanizması tesis eder. Şirket faaliyetlerine ve müşterilere ilişkin bilgilere erişilmesi, sorgulanması, bunlara yönelik erişim yetkilerinin verilmesi veya değiştirilmesine yönelik işlemler ve bunlara yönelik yetkisiz erişim teşebbüslerine ilişkin iz kayıtları tutulur.

Denetim izlerinin, bütünlüğünün bozulmasına, değiştirilmesine imkân vermeyecek şekilde ve raporlanabilir bir formatta tutulması esastır. Denetim izlerinin asgari 5 yıl süreyle denetime hazır bulundurulmasını sağlanır. Şirket kendisine ait dış hizmet sağlayıcı tarafından tutulan denetim izlerinin kendi Bilgi Güvenliği Politikası ve standartlarına uygun olarak saklanmasını sağlar.

Bilgi güvenliği yönetimi faaliyetleri sırasında kullanılacak denetim izi yönetimi süreci ***Denetim İzi Kayıtları Yönetimi Prosedürü*** dokümanında detaylandırılmıştır.

5.2.12. Yedekleme

Şirket; faaliyetlerini yürütmek için kullandığı sistem, veri tabanı ve uygulamaların yedeklerinin alınmasını ve periyodik yedekten geri dönüş testlerinin yapılmasını sağlar. Bilgi sistemleri yedekleme süreci ***Veri Yedekleme Prosedürü*** dokümanında detaylandırılmıştır.

5.2.13. Ağ Güvenliği

Ağ güvenliğinde Güvenlik Duvarı, IPS gibi katmanlı güvenlik mimarisi (bir güvenlik katmanının aşılması durumunda diğer güvenlik katmanının devreye girdiği) kullanılır. Uzaktan bağlantılarda VPN kullanılır. Şirket bilgi sistemleri ağ güvenliği süreci **Ağ Güvenliği Prosedürü** dokümanında detaylandırılmıştır.

5.2.14. Bilgi Güvenliği Siber Olay Yönetimi

Tüm Şirket çalışanları ve destek hizmeti veren kuruluşlar, bilgi güvenliğini tehlikeye atma ihtimali bulunan bir siber olay tespit etmeleri halinde bu olayı Bilgi Güvenliği Birimi'ne bildirmekle yükümlüdür. Bunun için uygun iletişim kanalları tesis edilir ve önceden bilgilendirmeler yapılır. Tespit edilen siber olaylara ilişkin

değerlendirmeler; Bilgi Teknolojileri Sorumlusu, Bilgi Güvenliği Sorumlusu ve ilgili diğer çalışanların katılımı ile değerlendirilerek asgari olarak yılda bir kez Üst Yönetim'e sunulur. Şirket' in siber olaylara müdahale süreci ***Siber Olaylara Müdahale Süreci Prosedürü*** dokümanında detaylandırılmıştır.

5.2.15. Yama Yönetimi

Bilgi Teknolojileri güvenlik seviyesinin mümkün olan en üst düzeyde kalması için güvenlik yamaları yönetiminde **Yama Yönetimi Prosedürü** dokümanında yer alan süreç işletilir.

Sistem yöneticileri ile görüşülerek yama ve yazılım versiyon uyum kararları konusunda karşılıklı olarak anlaşılır ve sene içerisinde bu kararlara uyum takip edilir. Yamaların yayınlanma sıklıklarına bağlı olarak yama uyum kararı; zamana, yamaya, versiyona ya da zafiyete göre takip edilir. Zafiyet üzerine yama seviyesi takip edilecek olan sistemlerin zafiyetleri düzenli yapılan sistem/network taramaları ile belirlenir ve yamaların geçilmesi için ilgili ekip bilgilendirilir.

5.2.16. Üçüncü Parti Hizmetlerinin Yönetimi

Tüm destek hizmet sözleşmeleri, yürürlükteki yasa ve düzenlemelere ilişkin gereklilikleri karşılayan hükümleri içerecektir. Üçüncü partiler tarafından sağlanan hizmetler, söz konusu hizmetlere ilişkin sözleşmelerde tanımlanmış olan uygun güvenlik kontrollerinin hayata geçirildiğinden emin olunması amacı ile düzenli olarak izlenecek, gözden geçirilecek ve denetlenecektir. Hizmetlerin sunulmasına ilişkin gerçekleştirilmek istenen büyük ya da küçük değişiklikler, etkilenecek sistem ve süreçlerin önemleri dikkate alınarak, ancak uygun yazılı iznin ardından hayata geçirilecektir.

6. Raporlama

Bilgi Güvenliği Sorumlusu tarafından yılda bir kez Yönetim Kuruluna sunulmak üzere; yetkisiz erişim teşebbüslerini, bilgi güvenliği sürecine uyum durumunu, bilgi güvenliği ihlaline ilişkin olayları içeren güvenlik ihlalleri raporu hazırlanır.

7. Sorumluluk

Bu politikanın hazırlanması, güncel tutulması ve uygulanmasından Bilgi Güvenliği Birimi sorumludur. Politika, en az yılda bir defa gözden geçirilir ve gerekli görüldüğü takdirde güncellenir.

8. Yürürlük

Bu politika, Yönetim Kurulu tarafından onaylandığı tarihte yürürlüğe girer ve güncellenmesi için de Yönetim Kurulu onayı gereklidir.

9. Doküman Tarihçesi

Tarih	Versiyon	Karar No	Açıklama
30.06.2026		YK-2026/11	İlk yayın.