HAYHAY FİNANSMAN A.Ş.

BİLGİ GÜVENLİĞİ POLİTİKASI

HAYHAY FİNANSMAN A.Ş.
BİLGİ GÜVENLİĞİ POLİTİKASI

1. Amaç:

Bu prosedürün amacı; Hayhay Finansman A.Ş. bünyesindeki bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutmaktır. Bilgi, işle ilgili diğer önemli varlıklar gibi bir kuruluşun faaliyetleri açısından gerekli olan ve bunun neticesinde de uygun bir şekilde korunması gereken bir varlıktır. Bilgi varlıklarının güvenliği Şirket tarafından tanımlanmış politikalar doğrultusunda sağlanır. Bilgi güvenliğinin amacı; bilgiye yetkisiz erişimin engellenmesi (Gizlilik), bilginin ve bilgi varlıklarının tam ve eksiksiz olması, doğru olması ve uygunsuz biçimde değiştirilmemesi (Bütünlük) ve yetkili kullanıcıların ihtiyaç duydukları veriye ihtiyaç duydukları zaman erişebilmesinin (Erişilebilirlik) sağlanmasıdır. Bilgi Güvenliği Politikası, Şirket'in tüm birimlerine ve hizmet sağlayıcılarına uygulanır. Şirket'in Bilgi Güvenliği Yönetim Süreci'nin hedefi Şirket tarafından üretilen, işlenen, saklanan bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak amacıyla bilgi varlıkları envanterini çıkarmak, risk değerlendirmesi yapmak, kontrolleri hayata geçirmek ve uygulanan kontrollerin etkinliklerini gözden geçirmektir.

2. Tanımlar:

Bilgi Güvenlik Komitesi (Komite): Bilgi sistemlerinin yönetimine ve bilgi güvenliğinin sağlanmasına ilişkin politikaların, prosedürlerin ve süreçlerin tesis edilmesi, bilgi teknolojilerinin kullanılmasından kaynaklanan risklerin etkin biçimde yönetilmesi amacıyla oluşturulan komiteyi,
Bilgi Güvenliği Yönetim Süreci: Olası risklerin ve tehditlerin belirlenmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetim eyleminin birbirini tamamlayacak şekilde gerçekleştirilmesidir.
Bilgi Sistemleri: Elektronik ortamda bilgilerin işlenmesi ve depolanması için kullanılan giriş, işleme, depolama, yedekleme, kopyalama ve yazdırma fonksiyonlarını kapsayan yazılım ve donanımlarını.
İş İstasyonu: Hayhay Finansman A.Ş. çalışanlarının bilgisayarlarını ifade etmektedir.
Şirket: Hayhay Finansman A.Ş.

3. Bilgi Sistemleri Yönetimine İlişkin Temel İlkeler

- Bilgi sistemlerinin yapısının, Şirket'in 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'le ilgili tüm bilgilerin yurt içinde elektronik ortamda güvenli ve istenildiği an erişime imkân sağlayacak şekilde saklanılmasına veya yedeklenmesine ve kullanılmasına,
    - Risk ölçüm yöntem veya modelleri kullanılarak risklerin ölçülebilmesine ve zamanında ve etkin bir şekilde raporlanabilmesine,
    - Önceden belirlenen risk limitlerine yaklaşılması halinde uyarıcı bilgiler üretilebilmesine,
    - Belirlenen azami risk düzeylerine ilişkin aşımların ve istisnaların zamanında raporlanabilmesine,

  - İki yılda bir Sızma yapılabilmesine,
  - Sunulan hizmet ve faaliyetlere ilişkin sermaye tahsisinin Şirket'in risk alma düzeyine göre belirlenmesine,
  - Muhasebe kayıtlarının Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu tarafından belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesine imkân verecek yapıda tesis edilmiştir.
- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere "Bilgi Sistemleri Süreklilik Planı" oluşturulmuştur. Söz konusu planın işlerliği ve yeterliliği düzenli olarak test edilmekte; ihtiyaç duyulması halinde gerekli tedbirler alınmaktadır. Bilgi Sistemleri sürekliliğinin planlanmasında, kritik bilgi teknolojileri varlıkları ile süreçleri belirlenmiştir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılmaktadır.
- Bilgi sistemleri ile içerdiği verinin güvenli biçimde saklanması esas alınmıştır. Bu çerçevede, veriler, güvenlik hassasiyet derecelerine göre sınıflandırılmaktadır, her bir sınıf için uygun düzeyde güvenlik kontrolleri tesis edilmiştir ve buna doğrultuda yedeklenmektedir. Bilgi sistemlerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilmekte ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler yapılmaktadır.
- Bilgi güvenliğinin temininde ve Şirket'in bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılmaktadır.
- Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanmaktadır. Bilgi sistemleri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları yazılı olarak belirlenmektedir. Görevler ayrılığı ilkesine uygunluk İç Kontrol Bölümü tarafından düzenli olarak test edilmekte; sonuçları Bilgi Güvenlik Komitesi Başkanı olarak Genel Müdür'e raporlanmaktadır.
- Faaliyetlerin yürütülmesi sırasında bilgi sistemleri aracılığıyla edinilen ve saklanan müşteri ve Şirket bilgilerinin gizliliğini sağlamak esastır. Müşteri bilgilerinin, yasalarla yetkili kılınmış merciler dışındaki taraflarla paylaşımına ilişkin uygulama esasları yazılı olarak belirlenmektedir.
- Bilgi sistemleri kullanılarak gerçekleştirilen ve şirket faaliyetlerine ait kayıtlarda değişikliğe neden olan işlemlere ilişkin olarak yeterli detayda ve açıklıkta denetim izleri tutulmaktadır. Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli tedbirler alınmıştır.
- Bilgi sistemleri faaliyetlerinde bilgi teknolojilerinin kullanılmasından kaynaklanan riskleri tespit etmek, analiz etmek, ölçmek, izlemek ve raporlamak üzere Risk Yönetimi Prosedürü oluşturulmuştur ve bu kapsamda alınacak dış hizmetlere ilişkin risklerde, süreç içerisine dâhil edilmiştir.
- Uygulamaya konulan bilgi sistemlerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenmektedir. Yeni bilgi sistemlerinin Şirket'te uygulanması, Şirket'in risk değerlendirmesi sürecine dâhil edilmektedir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri işleyişi yenilenmektedir.

4. Bilgi Güvenliği Rol ve Sorumluluklar

Bilgi Güvenliğinin Şirket'te planlanması, uygulanması ve kontrol edilmesi faaliyetlerini gerçekleştirmek amacıyla, Bilgi Güvenlik Komitesi, Bilgi Teknolojileri Bölümü ve Şirket çalışanları görev alır. Şirket Bilgi Güvenliği Politikası Bilgi Güvenliği Müdürü tarafından hazırlanır, Yönetim Kurulu tarafından onaylanır ve Bilgi Güvenlik Komitesi

tarafından yılda en az bir defa gözden geçirilir. Bilgi Güvenliği Politikası oluşturulurken Şirket'in güvenlik stratejisi, güvenlik gereksinimleri, yasal ve düzenleyici zorunluluklar göz önünde bulundurulmuştur. Bilgi Güvenlik Komitesi, Bilgi Güvenliği Politikasının hayata geçirilmesini sağlamaktadır. Şirket'in Bilgi Güvenliği Yöneticisi, Bilgi Güvenliği Müdürü'dür.

4.1. Bilgi Güvenlik Komitesi'nin Sorumlulukları:

Şirket'te bilgi teknolojileri risklerinin yönetiminden Bilgi Güvenlik Komitesi sorumludur. Komite Başkanlığını Genel Müdür yapar. Komite, toplantı esasıyla çalışmakta olup toplanma sıklığını ve koşullarını Komite Başkanı belirler. Komite'nin görevleri, "Bilgi Güvenlik Komitesi Görev Yönetmeliği'nde açıklanmıştır. Komite, Bilgi Güvenliği ile ilgili olarak;

- Bilgi Güvenliğinin uygulanacağı kapsamı belirler,
- Bilgi Güvenliği Politikasının belirlenmesini, Şirket çalışanlarına ve ilgili taraflara duyurulmasını sağlar,
- Risk değerlendirme yaklaşımını ve kabul edilebilir risk seviyelerini belirler,
- Risk değerlendirme Raporu sonuçlarını gözden geçirir, varsa bulgulara göre gerekli tedbirleri alır.
- Bilgi Güvenliği Planını onaylar, Bilgi Güvenliği Yönetim Süreci'ni gözden geçirir,
- Bilgi Güvenliği iç denetimlerinin gerçekleştirilmesini sağlar,
- İç denetim ve dış denetim sonuçlarını gözden geçirir, varsa bulgulara göre gerekli tedbirleri alır.
- Bilgi Güvenliği standartlarının belirlenmesini sağlar,
- Bilgi Güvenliği Yönetim Süreci'nin iyileştirilmesini sağlayacak önerileri ve ilgili tarafların geri bildirimlerini değerlendirir,
- Kritik bilgi sistemleri projelerini gözden geçirir, onaylar,
- Bilgi Güvenliği Yönetim Süreci'nin uygulanmasını etkileyebilecek olası değişiklikleri değerlendirir.
- Bilgi Teknolojileri Bölümü'nü, Bilgi Güvenlik Müdürü denetler.

Ayrıca Yönetim Kurulu'na sunulmak üzere; yetkisiz erişim teşebbüsleri, bilgi güvenliği uyum durumu, bilgi güvenliği ihlaline ilişkin olayları içeren güvenlik ihlalleri raporunun hazırlanması sağlanır. Bilgi Güvenlik Komitesi'nde görüşülen konular ve alınan kararları içeren toplantı tutanağı düzenlenir

4.2. Bilgi Teknolojileri Bölümü'nün Sorumlulukları:

- Komite ve Bilgi Güvenliği Müdürü tarafından öngörülen teknolojik ve idari güvenlik tedbirlerinin alınması,
- Şifre kullanımı ve denetimi, yetkilerin Genel Müdür onayı ile açılması, kullanıcı işlemlerinin kayıt altına alınması, yetkisiz erişim girişimi denetim izlerinin alınması,
- Sistem donanımları üzerindeki güvenlik uygulamalarının güncellik kontrolünün yapılması, Şirket tarafından kullanılmakta olan anti-virüs yazılımının bütün sunucu ve iş istasyonlarında yüklü olduğu ve çalıştığının takibi, düzenli olarak tarama ve güncelleme yapacak şekilde konfigüre edilmesi ve gözden geçirilmesi,
- Sistem üzerindeki tüm donanım ve yazılımlar üzerindeki kullanıcı hareketlerinin loglarının alınması, alınan raporların kontrol için Bilgi Güvenlik Koordinatörüne iletilmesi,
- Veri yedeklemelerinin ve yedekten geri dönüş testlerinin Yedekleme Prosedürüne uygun olarak yapılması yedekten dönüş uygunluğunun teyit edilmesi ve kayıtlarının

tutulması,
- Personelin Bilgi İşleme Cihazları Kullanımı kuralları, İnternet erişimi ve e-posta kullanımı kurallarına uyumunun denetlemesi,
- Genel Müdür tarafından uygun görülen ve onaylanan veri aktarımının veri güvenlik tedbirleri alınarak gerçekleştirilmesi, yapılan işlemlerin kayıtlarının tutulması,
- Veri Silme, İmha etme ve Anonimleştirme süreçlerinde yazılı prosedürlere uyulması, silinen yok edilen ve anonimleştirilen verilerin detaylarının arşivlenmesi

Bilgi Teknolojileri Bölümü'nün sorumluluğundadır.
Bilgi Teknolojileri Bölümü, görev alanına giren konularda Bilgi Güvenliği Müdürü tarafından denetlenir. Birimin tüm çalışanları anılan görevlerin yerine getirilmesinde müştereken sorumludur.

4.3. Bilgi Güvenliği Yöneticisinin Sorumlulukları:

Bilgi Güvenliği Müdürü aşağıdaki faaliyetleri gerçekleştirir:
- Bu politikada detayları anlatılan Bilgi Güvenliği Yönetim Süreci'nin kurulumuna yönelik çalışmaları organize eder ve yapılan çalışmalar hakkında Bilgi Güvenlik Komitesi'ni bilgilendirir,
- Varlık envanterinin çıkarılmasını ve risk değerlendirme çalışmalarını koordine eder,
- Gerekli politika, prosedür ve belgelerin oluşturulması çalışmalarına teknik destek verir,
- Bilgi Güvenliği projelerinin, hayata geçirilmesi çalışmalarını koordine eder,
- Yeni başlatılan veya devam eden projelerde bilgi güvenliğine yönelik gereksinimleri belirler,
- Risk analizi çalışmalarını koordine eder,
- Bilgi güvenliğinin izlenmesine yönelik faaliyetleri koordine eder,
- Bilgi güvenliğini etkileyen, iç ve dış mevzuata uyum çalışmalarını koordine eder,
- Bilgi Güvenliği Politikasının herkese bildirilmesi ve uygulanması için gerekli mekanizmaların kurulması ve personele farkındalık eğitimi verilmesine teknik destek verir, bilgi güvenliğine yönelik eğitim ihtiyaçlarını belirler,
- Meydana gelebilecek bilgi güvenlik saldırılarının takip edilmesini, gerekli önlemlerin alınmasını ve raporlanmasını koordine eder,
- Bütçe hazırlama döneminde güvenlik ile ilgili bütçenin hesaplanmasına destek verir,
- Bilgi varlıklarına ait risklerle ilgili konularda gerektiğinde Yönetim Kuruluna ve Üst Yönetime danışmanlık yapar.
- Geliştirilen yazılımlara yönelik güvenlik standartlarını belirler,
- Düzeltici ve önleyici faaliyetlerin yapılması gereken bilgi güvenliği olayları için gerçekleştirilen düzeltici ve önleyici faaliyetlerin sonuçlarını izler, alınan aksiyonların etkinliğini gözden geçirir,
- Tekrar eden ve kritik olan bilgi güvenliği olaylarının kök nedenlerinin tespit edilmesini ve gerekli önlemlerin alınmasını sağlar.
- Bilgi Güvenliği Politikasını yılda en az bir kere gözden geçirir ve güncellenmesi durumunda Bilgi Güvenlik Komitesi'nin onayına sunar.

4.4. Altyapı ve Güvenlik Müdürünün Sorumlulukları:

Altyapı ve Güvenlik Müdürü, Bilgi Teknolojileri Yöneticisine bağlı olarak aşağıdaki faaliyetleri gerçekleştirir:
- Tanımlanmış olan güvenlik standartlarının gereklerini sistemler üzerinde uygulamaya koyar,

- Yeni başlayan veya devam eden projelerde belirlenmiş olan güvenlik gerekliliklerini uygular,
- Sorumluluğu altındaki güvenlik sistemleri üzerindeki operasyonları gerçekleştirir,
- Değişen teknolojiler veya güvenlik tehditlerine karşı güvenlik sistemleri üzerindeki güncelleme ve yükseltme çalışmalarını gerçekleştirir,
- Kurumun dış dünyaya açılan hizmetlerinin güvenli bir şekilde sunulmasını sağlar,
- Tespit edilen güvenlik tehditlerini ve ihlallerini ilgili taraflara bildirir,
- Sorumluluğu altındaki sistemlerde gerçekleşen bilgi güvenliği olaylarının tekrar etmesini engelleyecek aksiyonları alır,
- Sorumluluğu altındaki güvenlik sistemleri üzerindeki güvenlik seviyesinin artırılmasına yönelik gereklilikleri üstlerine raporlar.

4.5. Yazılım Geliştirme ve Analiz Müdürünün Sorumlulukları

- Yazılım geliştirme ve BT altyapı stratejilerini belirlemek, şirketin genel hedeflerine uygun planlamalar yapmak,
- Dijital dönüşüm, otomasyon ve teknoloji yatırımlarında yön gösterici rol üstlenmek,
- Ekiplerin görev dağılımını yapmak, performanslarını takip etmek ve gelişimlerine destek olmak,
- DevOps süreçlerini denetlemek ve iyileştirmek,
- Yeni yazılım çözümlerinin analiz, tasarım, geliştirme ve test süreçlerini denetlemek,
- Kod kalitesi, sürdürülebilirlik ve ölçeklenebilirlik konusunda standartlar belirlemek ve uygulanmasını sağlamak,
- Sunucu, ağ, veritabanı, bulut servisleri, güvenlik ve diğer altyapı bileşenlerinin yönetiminden sorumlu olmak,
- BT altyapısının sürekliliğini, performansını ve güvenliğini sağlamak,
- Yedekleme, felaket kurtarma ve iş sürekliliği planlarını oluşturmak ve uygulamak.

4.6. Şirket Çalışanlarının Sorumlulukları:

- Şirket çalışanları kendilerine tahsis edilmiş iş istasyonunda bulunan Şirkete özel bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak için azami özeni gösterir.
- Şirket çalışanları Bilgi Teknolojileri Bölümü'nün hazırladığı iş istasyonu sistem konfigürasyonunu değiştiremezler.
- Şirketin Bilgi Sistemleri Politikasında Şifre Kullanımı, İnternet Erişimi, E-posta Kullanımı, Bilgi İşleme Cihazları Kullanımı, Şirket Verilerinin Güvenli Kullanımı, Fiziksel Güvenlik Kontrolleri, Sistem Donanımları Güvenliği, Sosyal Mühendislik, Kaydedici Cihazlar Kullanımı, Yazılım Kullanımı, Bilgi Güvenlik Olaylarının Bildirimi ve Bilgi Güvenliği Politikasına Uyum başlıkları altında belirlenen kurallara uymak zorundadırlar.
- Kendi görev alanları çerçevesinde yeni ortaya çıkan veya değişen riskleri, şirketin ilgili politika, prosedür ve yönetmelikleri ile belirlenen yetki ve sorumlulukları çerçevesinde tespit eder, tanımlar, değerlendirir, gözden geçirir ve gereğinde Bilgi Teknolojileri Bölümü'nü bilgilendirir. Böylece, risk yönetimi süreçlerine doğrudan katkıda bulunurlar.

5. Bilgi Güvenlik Yönetimi Süreçleri

5.1. Bilgi ve Veriyi Sınıflandırma

Bilgiyi Tanımlama
Şirket içinde kullanılan ve saklanan bilgilere ait detaylı ve güncel bir envanter listesi tutulur. Bu envanter listesi senede bir defa mutlaka güncellenir.
Bilgiyi Sınıflandırma
Tüm bilgi, veri ve dokümanlar kendi gizlilik, hassasiyet, değer ve kritiklik seviyelerine göre sınıflandırılırlar.
Sınıflandırılmış Bilginin Sahipliğinin Kabulü
Her bir bilgi, veri ve doküman kalemi için belirlenmiş bir veri sahibi vardır.
Sınıflandırılmış Bilgiyi Etiketleme
Tüm bilgi, veri ve dokümanlar gizlilik derecesine göre etiketlenirler ve bu sayede tüm kullanıcılar sahiplik, sınıflandırma ve bilginin değeri gibi kavramların farkındadırlar.
Sınıflandırılmış Bilgiyi Saklama ve Yürütme
Tüm bilgi, veri ve dokümanlar kendilerine ait bütünlüğü ve gizliliği korumak için sınıflandırılır ve bu şekilde işlenmek üzere saklanırlar.
Çok Gizli Bilgiyi İzole Etmek
Tüm çok hassas bilgi, veri ve dokümanlar güvenli bir yerde saklanır.
Ağ Güvenliği Yönetimi
Şirket ağı üzerinden veriye erişim kabul görmüş sıkı güvenlik kriterleri üzerinden sağlanır ve bu kriterler sıklıkla değerlendirilip güncellenirler.

5.2. Bilgi Varlıklarının Yönetimi

Basılı ve dijital ortamda oluşturulan, iletilen, saklanan veya sözlü olarak paylaşılan Şirket'e ait tüm veriler Şirket bilgi varlıkları kapsamına girer ve süreç Veri Sınıflandırma Prosedürü içerisinde tanımlanmıştır. 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 varlık değerlendirmelerini yaparak bilgi varlıklarını Varlık Envanteri dokümanı içerisinde sınıflandırmıştır. Şirket bilgilerinin bu sınıflandırmaya uygun olarak kullanılmasını sağlar. Her varlığa bir sahip atanmış ve varlıklarla ilgili sorumluluklar bu sahipler üzerine verilmiştir.

5.3. Risklerin Yönetimi

Şirket'in bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Bilgi Güvenlik Komitesi tarafından belirlenmiştir ve Risk Yönetimi Prosedürü içerisinde tanımlanmıştır. Bilgi güvenliği risk değerlendirme yaklaşımı ile Şirket'in bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği ilgili prosedür içerisinde belirlenmiştir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilmektedir.

5.4. Bilgi Güvenliği Farkındalığı Yaratılması

Şirket, bütün personeli için farkındalık eğitim gerekliliklerini belirlemiş ve personeline buna uygun bir şekilde yılda bir kez bilgi güvenliği eğitimi sağlamaktadır. İşe yeni alınan tüm çalışanlar bilgi güvenliği konusunda bilgilendirilmektedir. Şirket, kendi çalışanlarına işe giriş esnasında ve tedarikçi şirket çalışanlarına çalışmaların başında bilgi güvenliği politikalarını bildiklerine ve uyacaklarına dair imzalı onaylarını almaktadır.

5.5. Kimlik Yönetimi, Yetkilendirme ve Şifre Yönetimi

Şirket'in personelinin kimlik yönetimi, yetkilendirme süreci ve şifre yönetimine ilişkin yaklaşımı Kimlik Yönetimi ve Yetkilendirme Prosedürü içerisinde tanımlanmıştır.

5.6. Ağ Güvenliği Politikası

- Şirket firewall olarak Fortigate firewall yazılımı kullanmaktadır. Fortigate üzerinde belirlenen kurallar sistemin dış etkenlerden gelen saldırılara karşı korunmasını sağlamaktadır.
- Şirket personeli TCP/IP protokolünü kullanarak sadece HTTP, HTTPS kullanarak İnternet erişimi sağlayabilirler. FTP, ROP, TELNET ve ONS servislerine sadece Bilgi İşlem Bölümü çalışanları erişebilmektedir.
- Şirket çalışanlarının HTTP, HTTPS kullanarak yaptıkları İnternet bağlantılarından gelebilecek virüs tehditlerini engellemek için antivirüs ve EDR kullanılmaktadır.
- Mail sistemindeki saldırıları engellemek için Mail Gateway programı kullanılmaktadır.
- Şirkette Bilgi İşlem Bölümü tarafından düzenli aralıklarla İç Sızma testleri yapılmaktadır.
- Şirkette, Dış Sızma Testi, 2 yılda bir Dış Hizmet alınan bir kuruluşa yaptırılmaktadır.

5.7. Bilgi Sistemleri Süreklilik Yönetimi

Şirket'in bilgi sistemlerine ilişkin süreklilik yönetimine ilişkin yaklaşımı Bilgi Sistemleri Süreklilik Planı içerisinde tanımlanmıştır.

5.8. Kullanıcı İşlemlerinin Kayıt Altına Alınması

Şirket çalışanlarının bilgi sistemleri dâhilinde gerçekleştirdikleri finansal ya da operasyonel işlemlerin başlangıcından bitimine kadar takip edilebilmesini sağlayacak denetim izi kayıtları saklanır. Şirket'in denetim izlerinin yönetimine ilişkin yaklaşımı Denetim İzlerinin Yönetimi Prosedürü içerisinde tanımlanmıştır.

5.9. Uygunsuz Kullanım

- Şirket'in bilgi sistem kaynakları hiçbir şekilde yasa dışı amaçlar için kullanılamaz.
- Bilgi sistem kaynakları, Şirket'in çıkarlarıyla çelişen ve Şirket'in normal

operasyon ve iş aktivitelerini engelleyici aktiviteler için kullanılamaz.

- Şirket'in hizmet verdiği ortamlarda Şirket'e ait bilgisayarlar ile sadece Şirket'in sağlamış olduğu İnternet erişim kaynakları kullanılabilir, üçüncü kişilerin sağlamış olduğu kablosuz ağlara bağlanılamaz, dial-up bağlantı gerçekleştirilemez.
- İnternet erişimi ile Şirket çıkarlarıyla çelişebilecek ve Şirket'in operasyonlarını ve faaliyetlerini olumsuz olarak etkileyebilecek işlemler gerçekleştirilemez.
- İnternet erişimi aracılığı ile lisanssız yazılım kullanımı, fikir ve sanat eserlerine izinsiz erişim, çoğaltma ve paylaşma gibi telif hakkı ihlali içeren işlemler gerçekleştirilemez.
- İnternet erişimi, uygunsuz içeriği saklamak, bağlantı olarak vermek, erişmek ve göndermek için kullanılamaz.
- İnternet erişimi, kişisel çıkar sağlama amaçlı olarak kullanılamaz.
- Şirket'in sağlamış olduğu kablosuz İnternet erişim şifre bilgileri danışmanlar, hizmet sağlayıcılar ve misafirler haricindeki üçüncü taraflarla paylaşılamaz.
- Çalışanlar internetin sağladığı tartışma, haber panoları ve sohbet odalarına kurumsal kimlikleri ile katılamazlar.
- Kullanıcılar, e-posta ile uygun olmayan içerikte (ırkçılık, siyasi propaganda, ahlak dışı ifadeler vb.) mesajlar gönderemez ve bu tür mesajlara cevap veremezler. E-posta kullanımı için tanımlanmış olan Outlook uygulaması dışında başka bir uygulama kullanılamaz.
- E-posta ile paylaşılamayacak gizlilik seviyesindeki bilgiler gizlilik anlaşması imzalanmamış üçüncü taraflar ile e-posta üzerinden paylaşılamaz.
- Kişisel amaçlı kullanılan İnternet sitelerine kurumsal e-posta adresi ile üye olunamaz, bu sitelere kurumsal e-posta adresinden e-posta gönderilemez.
- Bilgiyi işlemeye, saklamaya ya da bilgiye erişmeye yarayan cihazlar, şirket çalışanlarına iş amaçlı olarak sağlanmıştır, çalışanlar bu cihazlar üzerinde izin verilenler haricinde değişiklikler yapamaz.
- Ortak kullanım amacı ile tahsis edilmiş olan cihazlar üzerinde hassas kurum bilgileri bırakılamaz.
- Şirket ve faaliyetleri ile ilgili herhangi bir bilgi veya veri, izin verilenler dışında harici cihazlar üzerinde saklanamaz.

6. Yürürlük

Yönetim Kurulu tarafından onaylandığı tarih itibariyle yürürlüğe girer.