POFİNTECH ÖDEME HİZMETLERİ VE ELEKTRONİK PARA ANONİM ŞİRKETİ BİLGİ GÜVENLİĞİ POLİTİKASI

İşbu Şikayet Yönetimi Politikası, **POFintech Ödeme Hizmetleri ve Elektronik Para Anonim Şirketi** ("**Şirket**") tarafından işletilen www.vinss.com.tr alan adlı internet sitesini ve Şirket'e ait mobil uygulamayı (internet sitesi ve uygulama birlikte **"Platform"** olarak anılacaktır) kullanan ziyaretçiler ("**Kullanıcı**") için geçerlidir ve Şirket'in bilgi güvenliği politikasının oluşturulması kapsamında hazırlanmıştır.

1. AMAÇ VE KAPSAM

Bu politikalar dokümanı, Şirket bünyesindeki bilgi sistemlerinin ve verilerin gizlilik, bütünlük ve erişilebilirliğini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözetim altında tutmayı amaçlar.

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 ile İlgili Politikalar, 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.

Bu doküman tavsiyelere, kanunlara, yönetmeliklere uygun ve uluslararası standartları temel alarak kontrol alt yapısını geliştirmek ve düzenli olarak güncellenecektir.

2. TANIMLAR VE KISALTMALAR

6493 Sayılı Kanun:	: Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun'u ifade eder.
Bilgi Güvenliği Komitesi	: 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 ifade eder.
Hassas müşteri verisi	: Ödeme emrinin verilmesinde veya müşterinin kimliğinin doğrulanmasında kullanılan ve üçüncü kişilerce ele geçirilmesi veya değiştirilmesi halinde dolandırıcılık ya da müşteri adına sahte işlem yapılmasına imkan verebilecek kişisel veriler ile müşteri güvenlik bilgilerini ifade eder.
Şirket	: POFintech Ödeme Hizmetleri ve Elektronik Para Anonim Şirketi'ni ifade eder.
Tebliğ	: Ödeme ve Elektronik Para Kuruluşlarının Bilgi Sistemleri ile Ödeme Hizmeti Sağlayıcılarının Ödeme Hizmetleri Alanındaki Veri Paylaşım Servislerine İlişkin Tebliğ'i ifade eder.
Yönetmelik	: Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Hizmeti Sağlayıcıları Hakkında Yönetmelik'i ifade eder.

3. BİLGİ SİSTEMLERİ YÖNETİMİNE İLİŞKİN 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,
    - Sızma ve stres testi yapılabilmesine,
    - Muhasebe kayıtlarının Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurulu tarafından belirlenen usul ve esaslara uygun şekilde muhasebeleştirilmesine,
    - imkân verecek yapıda tesis edilir.
- Bilgi sistemlerinin sürekli biçimde işlerliğini sağlamak üzere iş sürekliliği planı oluşturulur. Söz konusu planın işlerliği ve yeterliliği düzenli olarak test edilir; ihtiyaç duyulması halinde gerekli tedbirler alınır. İş sürekliliğinin planlanmasında, kritik bilgi

teknolojileri varlıkları ile süreçleri belirlenir; bunlara ilişkin iş etki analizi ile risk değerlendirmesi yapılır.

- 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 sistemlerinin güvenliği ve yedekleme sistemlerinin işleyişi düzenli olarak test edilir ve test sonuçlarına göre ihtiyaç duyulması halinde gerekli değişiklikler yapılır.

- POFintech Ödeme Hizmetleri ve Elektronik Para A.Ş., elektronik kanal üzerinden sunduğu hizmetlere ilişkin tüm yazılım ve mobil uygulamaların bilgi güvenliğini tehlikeye sokacak hususlar içermemesini sağlayacak gerekli teknik ve idari önlemleri almıştır. Güvenlik açıklarını giderecek gerekli yamaları ve güncellemeleri periyodik olarak sağlamaktadır.

- Bilgi güvenliğinin temininde ve Şirket'in bilgi sistemlerine erişimde, kimlik doğrulama ve yetkilendirme mekanizmaları ile inkâr edilemezlik ve sorumluluk atama imkânlarını içeren teknikler kullanılır.

- Bilgi sistemlerinin geliştirilmesi, test edilmesi ve işletilmesi süreçlerinde görevler ayrılığı ilkesi uygulanır. Bilgi sistemleri yönetim sürecinde görev alan bölüm ve çalışanların görev, yetki ve sorumlulukları yazılı olarak belirlenir. Görevler ayrılığı ilkesine uygunluk düzenli olarak test edilir; sonuçları Risk ve Uyum Yöneticisine raporlanır.

- 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 belirlenir.

- Bilgi sistemleri kullanılarak gerçekleştirilen 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 sistemleri yönetimi kapsamında alınacak Dış hizmetlerine ilişkin risk analizi yapılır.

- Uygulamaya konulan bilgi sistemlerinin işleyişi, stratejik hedeflere uygunluğu, kontrollerin etkinliği ve yeterliliği, bilgi teknolojilerindeki gelişmeler de göz önüne alınarak düzenli olarak izlenir. Yeni bilgi sistemlerinin Şirket'te uygulanmasının, Şirket'in risk profili üzerinde yaratacağı etki değerlendirilir. Bu çerçevede, gerek duyulması halinde, bilgi sistemleri işleyişi revize edilir.

- Kişisel bilginin mahremiyetinin korunmasını sağlamak amacıyla müşteri ve personel bilgilerinin gizliliğini korur.
- Bilginin bütünlüğünü koruyacak ve sürekli erişilebilirliğini garanti altına alacak altyapıyı ve kontrolleri hayata geçirir.
- Tasarım, geliştirme, test ve uygulama süreçlerinde görevler ayrılığı prensibine uygun yetkilendirmeyi sağlar ve kritik işlemlerde onay mekanizması tesis eder.
- Geliştirme, Test ve Üretim ortamlarının fiziksel ve mantıksal olarak ayrılmasını sağlar.
- Kullanıcıların yetkilendirilmesinde gerekli olan minimum yetkilendirme prensibinin sağlanması ve yetkilerin düzenli olarak kontrol edilmesini sağlar.
- Dış ağlardan gelebilecek tehditlere karşı ağ güvenliğini tesis eder.
- Katmanlı güvenlik mimarisini tesis eder ve sürekli gözetimini sağlar.
- Hassas müşteri verilerinin ve kişisel bilgilerin iletilmesinde ve saklanmasında şifreleme, maskeleme gibi güvenliği sağlayacak tedbirlerin alınmasını sağlar.
- Kullanılan şifreleme anahtarlarının güvenilirliğini sağlar.
- Bilgi güvenliği faaliyetlerinin yönetilmesini ve koordinasyonunu sağlamak amacıyla bir bilgi güvenliği organizasyonu oluşturur.
- Bilgi varlıkları envanterini çıkarır, sahiplikleri belirler ve bilgi varlıkları üzerindeki riskleri yönetir.
- Bilgi güvenliği olaylarının tespit edilmesi, raporlanması ve tekrarının önlenmesi adımlarını içeren bilgi güvenliği olay yönetimi faaliyetleri gerçekleştirir.
- Tüm personele yeterli seviyede farkındalık programı uygular ve bilgi güvenliği gerekliliklerinin karşılanması için tüm çalışanların katılımını sağlar.
- Bilginin işlendiği alanlarda bilginin güvenliğinin sağlanabilmesi amacıyla gerekli fiziksel ve çevresel güvenlik önlemlerini alır.
- Bilgi sistemleri edinim, geliştirme ve bakımında güvenlik gerekliliklerinin neler olduğunu belirler ve hayata geçirir.
- Belirlenen bilgi güvenliği politikalarına, süreçlerine, yasal ve düzenleyici zorunluluklara çalışanların uymalarını yazılı taahhütlerini alarak zorunlu tutar.
- İş faaliyetlerindeki kesintileri önlemek ve bilgiye sürekli erişimi sağlamak için iş sürekliliği faaliyetleri gerçekleştirir.
- Bilgiye erişimi kontrol etmek ve yetkisiz erişimleri önlemek için ilgili tüm alanlarda gerekli güvenlik kontrollerini hayata geçirir.
- Bilgi sistemleri faaliyetlerinin işletilmesinde gerekli güvenlik kontrolleri uygular, buna yönelik rol ve sorumlulukları tanımlar.

4. BİLGİ GÜVENLİĞİ ROL VE SORUMLULUKLARI

Bilgi Güvenliğinin Şirket'te planlanması, uygulanması ve kontrol edilmesi faaliyetlerini gerçekleştirmek amacıyla, Bilgi Sistemleri Müdür ve Şirket çalışanları görev alır. İlgili tarafların bu kapsamdaki görev ve sorumlulukları *Bilgi Güvenliği Rol ve Sorumluluklar Yönetmeliği'*nde açık olarak tanımlanır. Şirket *Bilgi Güvenliği Politikası* Bilgi Güvenliği Uzmanı tarafından hazırlanır, Risk ve Uyum Birimi tarafından yılda en az bir defa gözden geçirilir ve Yönetim Kurulu tarafından onaylanır. *Bilgi Güvenliği Politikası* oluşturulurken Şirket'in güvenlik stratejisi, güvenlik gereksinimleri, yasal ve düzenleyici zorunluluklar göz önünde bulundurulur. Şirket Yönetim Kurulu *Bilgi Güvenliği Politikasının* hayata geçirilmesini sağlar.

4.1. Bilgi Varlıklarının Yönetimi

Basılı ve dijital ortamda oluşturulan, iletilen, saklanan veya sözlü olarak paylaşılan Şirket'e ait tüm veriler Şirket bilgi varlıkları kapsamına girer. 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 sınıflandırır. Şirket bilgilerinin bu sınıflandırmaya uygun olarak kullanılmasını sağlar. Her varlığa bir sahip atanır ve varlıklarla ilgili sorumluluklar bu sahipler üzerine verilir.

4.2. Risklerin Değerlendirilmesi

Şirket'in bilgi güvenliğine ilişkin risk değerlendirme yaklaşımı Risk ve Uyum Birimi tarafından belirlenir ve *Bilgi Güvenliği Yönetim Süreci* kapsamında tanımlanır. Bilgi güvenliği risk değerlendirme yaklaşımı ile Şirket'in bilgi güvenliği risklerinin hangi yöntemler ile belirleneceği, risk seviyelerinin nasıl hesaplanacağı ve risklerin nasıl değerlendirileceği belirlenir. Bilgi varlıklarıyla ilgili oluşabilecek risklerin tanımlanması, derecelendirilmesi, işlenmesi ve gözden geçirilmesi çalışmaları belirlenen risk değerlendirme yaklaşımına uygun olarak gerçekleştirilir.

Risk değerlendirme çalışması sonucunda, riskleri azaltmaya yönelik aksiyonları içeren Şirket *Bilgi* Güvenliği Planı oluşturulur. Bilgi Güvenliği Planı yıllık olarak oluşturulur ve güncellenir.

Bilgi güvenliği yönetim sisteminde, personelin işe başlaması, görev ve pozisyon değiştirmesi ve işten ayrılması da dahil olmak üzere personele ilişkin tüm hususlar bilgi güvenliğini etkileyen yönleriyle değerlendirilir ve gerekli tedbirler alınır.

4.3. Güvenlik Farkındalığı Yaratılması

Kuruluş, bütün personeli için farkındalık eğitim gerekliliklerini belirler ve personeline buna uygun bir şekilde eğitim sağlar. İşe yeni alınan her çalışanlar bilgi güvenliği konusunda bilgilendirilmelidir. Şirket, kendi çalışanlarına ve tedarikçi şirket çalışanlarına bilgi güvenliği politikalarını bildiklerine ve uyacaklarına dair imzalı onaylarını alır.

Kuruluş, telefonda verdiği hizmetlerin müşterilere sunulmasında görev alan personele sosyal mühendislik saldırıları ve bilinen diğer dolandırıcılık yöntemleri konusunda periyodik eğitimler aldırmak ve bu çalışanların güvenlik farkındalıklarını artırıcı çalışmalar yapmakla yükümlüdür

4.4. Fiziksel ve Çevresel Güvenlik

Şirket *BS Fiziksel Çevre Yönetim Prosedürü* kapsamında bilgi işleme faaliyetlerinin gerçekleştiği binalara, alanlara yetki dışı fiziksel erişimi, müdahale ve hasarı engellemek amacı ile fiziksel güvenlik önlemleri alır. Bilgi işleme faaliyetlerinde kullanılan teçhizata yönelik güvenlik kontrolleri uygulanarak bilgi varlıklarının kaybı, hasarı, çalınması, tehlikeye girmesi ve kuruluşun faaliyetlerinin kesintiye uğraması engellenir. Ayrıca şirket üçüncü partilerden hizmet aldığı durumlarda hizmet alınan firmanın şirketin fiziksel ve çevresel güvenlik kriterlerine uygunluğunu kontrol etmelidir.

4.5. Haberleşme ve İşletim Yönetimi

Bilginin işlendiği tesislerin, ortamların ve araçların amacına uygun ve güvenli bir şekilde işletilmesini ve yönetilmesini sağlamak amacıyla süreçler oluşturulur, sorumluluklar tanımlanır.

Süreçlere yönelik sorumluluklar tanımlanırken bir işi yapan rol ile yapılan işi denetleyen rol aynı kişiye verilmez.

Yazılım ve bilginin bütünlüğünü korumak amacıyla kötü niyetli kodlara ve uygulamalara karşı güvenlik kontrolleri gerçekleştirilir. Bilginin ve bilgi varlıklarının bütünlüğünü ve kullanılabilirliğini sağlamak için yedekleme faaliyetleri gerçekleştirilir.

Ağdaki bilginin ve destekleyici altyapının korunmasını sağlanır.

Varlıkların yetkisiz ifşa edilmesi, değiştirilmesi, kaldırılması veya yok edilmesini ve iş faaliyetlerinin kesintiye uğramasını önlemek amacıyla bilginin işlenmesine, yönelik standartlar *Veri Sınıflandırma* kılavuzu kapsamında oluşturulur.

Dış kurumlarla veya Şirket içerisinde alınıp verilen bilgi ve yazılımın güvenliğini sağlayacak güvenlik kontrolleri uygulanır.

İnternet sitesi hizmetlerinin güvenlik gereklilikleri sağlanır.

Yetkisiz bilgi işleme faaliyetlerini algılamak amacıyla bilgi sistemleri uygulamalarına yönelik denetim izleri oluşturulur ve izleme faaliyetleri *Denetim İzlerinin Oluşturulması ve İzleme Prosedürü* kapsamında gerçekleştirilir. Denetim izleri anlık olarak alınır ve herhangi bir anomalinin yaşanmadığına dair bilgilendirmeler için aylık olarak IBM QRADAR üzerinden kontrol edilir.

Yılda en az bir kere yetkin ve bağımsız bir dış şirket tarafından sızma testleri yapılır. POFintech Ödeme Hizmetleri ve Elektronik Para A.Ş., elektronik kanal üzerinden sunduğu hizmetlere

ilişkin tüm yazılım ve mobil uygulamaların kaynağının kendisi olduğunun müşteri tarafından doğrulanabilmesini sağlamıştır. Kuruluş, e-posta sunucusuna gelen ve giden e-postaları tarayarak zararlı yazılım barındıran ya da kuruluşun iş ihtiyaçları doğrultusunda gereksiz olan eklentiler içeren e-postaları engelleyecek çözümler kullanır.

Kuruluştan gönderilen e-postalar için e-posta sunucularında gönderici kimliğini doğrulayıcı teknikler kullanılır.

4.6. Erişim Kontrolü

Bilgiye erişimi kontrol etmek için kullanıcı erişimleri güvenlik gereksinimlerini temel alacak şekilde yönetilir ve yetkisiz erişimler önlenir. Kabul edilebilir kullanım gereksinimleri *Kabul Edilebilir Kullanım Politikası*nda belirlenir ve kullanıcılara bildirilir. Erişim yetkileri görevler ayrılığı ilkesine ve gerekli olan minimum yetkilendirme prensibine uygun olarak sağlanır. Yetkiler düzenli olarak gözden geçirilir. Ağ erişimlerine yönelik güvenlik kontrolleri ile ağ bağlantılı hizmetlere yetkisiz erişimler engellenir. İşletim sistemlerine ve uygulamalara yönelik erişim kontrolleri hayata geçirilir. Mobil bilgi işleme ve uzaktan çalışma hizmetlerini kullananlar için bilgi güvenliği gereksinimleri karşılanır ve uzaktan bağlantı durumlarında uçtan uca güvenlik sistemi tesis edilir. POFintech Ödeme Hizmetleri ve Elektronik Para A.Ş.'nin bilgi sistemleri unsurları, bu unsurlara taşınabilir bir medya veya harici cihaz takıldığında otomatik olarak içeriği oynatmayacak şekilde yapılandırılmıştır ve zararlı yazılım engelleme araçları bu tür cihazlar takıldığında otomatik olarak bu cihazları tarayacak şekilde ayarlanmıştır. Bunun yanında bu tür harici cihazların bağlanacağı bağlantı ara yüzlerinin ön tanımlı olarak kullanıma kapatılarak bu tür cihazların kullanımının yalnızca iş gereksinimi olan personelle sınırlı tutulması ve harici cihazları kullanma denemesi yapılan durumların da takip edilmesi sağlanır.

4.7. Ağ Güvenliği

Ağ trafiğinde güvenliği sağlamak amacıyla, ağ kontrol güvenlik sistemleri bulunur. Ağ güvenliğinde dış güvenlik duvarı, IPS, iç güvenlik duvarı, SSM gibi katmanlı güvenlik mimarisi (bir güvenlik katmanının aşılması durumunda diğer güvenlik katmanının devreye girdiği) kullanılır.

Ağ güvenliğinde kullanılan sistemler, sürekli gözetim altında tutulur. Dış ağ ile kurulan bağlantılarda VPN ve SSL kullanılır.

POFintech Ödeme Hizmetleri ve Elektronik Para A.Ş., iç ve dış ağlar arasında Kanun kapsamındaki faaliyetler ile ilgili gerçekleşen her türlü iletişim sürecinin ve ana faaliyetlerine ilişkin operasyonel işlemlerin, güvenlik kontrolleri ve araçları kullanılarak gerçekleşecek şekilde tasarlanmasını sağlamıştır.

Kuruluş, iç ağdan gelebilecek tehditlerin etkisini azaltmak ve iç ağın farklı güvenlik hassasiyetine sahip alt bölümlerini birbirinden ayırarak kontrollü geçişi temin etmek üzere ağ segmentasyonu yapar.

İç ağdaki her bir servise ilişkin trafiğin yalnızca kendisi için gerekli olan ağ segmentlerine ulaşması, farklı ağ segmentleri arasındaki veri trafiğinin güvenliği ve iç ağa sadece yetkilendirilmiş cihazların bağlanması sağlanır.

Kritik ağ segmentlerine yapılan bağlantılar düzenli olarak tespit edilerek bu bağlantıların her biri için gereksinim değerlendirmesi yapılır ve gereksiz bağlantıların sonlandırılması sağlanır.

Kuruluş, kullanmakta olduğu veya ihtiyaç duyabileceği uygulamalar için bir beyaz liste oluşturur ve bilgi sistemleri unsurlarında sadece ihtiyaç duyulan uygulamaların yüklü olmasını sağlar, bu unsurlara beyaz liste dışındaki uygulamaların yüklenmesini ve bu uygulamaların çalıştırılmasını engelleyecek önlemleri alır. Kuruluş, bilgi sistemleri unsurları üzerinde beyaz listede yer almayan herhangi bir uygulamanın yüklü olup olmadığına yönelik düzenli olarak tarama gerçekleştirir.

Hassas müşteri verileri veya müşteri bilgilerine sahip sistemlerin özel iç ağda bulunması ve hiçbir şekilde doğrudan internetten erişilemiyor olması sağlanmıştır.

4.8. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı

Gerçekleştirilen bilgi sistemleri edinim, geliştirme ve bakımı operasyonlarında güvenlik gereksinimleri uygulanır. Uygulamalardaki bilginin bozulmasının, kaybının, yetkisiz değiştirilmesinin ve kötüye kullanımının önlenmesi için kontroller hayata geçirilir. Sistem dosyalarının ve sistem verilerinin güvenliğini sağlamak amacıyla güvenlik kontrolleri uygulanır. Uygulamalar ve sistemler üzerinde yapılacak değişiklikler ile kontrollü olarak gerçekleştirilir ve güvenlik riskleri azaltılır. Dışarıdan sağlanan yazılım geliştirmelerinin bilgi güvenliği gereksinimlerini sağlaması temin edilir.

4.9. Bilgi Güvenliği Olayları Yönetimi

Bilgi sistemleri ile ilişkili bilgi güvenliği olayları, ihlalleri ve zayıflıkları *Bilgi Güvenliği Olay Yönetim Süreci* kapsamında raporlanır. Raporlama düzeltici önlemlerin zamanında alınabilmesini sağlayacak şekilde gerçekleştirilir. Tüm çalışanların, tedarikçilerin ve üçüncü taraf kullanıcıların bilgi güvenliği olaylarının raporlanmasına katılımı sağlanır. Olayların sonucunda iyileştirici faaliyetler hayata geçirilir tekrar eden olayların önüne geçilir.

4.10. Bilgi Sistemleri Sürekliliği Yönetimi

İş faaliyetlerindeki kesilmeleri önlemek, önemli iş süreçlerini bilgi sistemleri aksaklıklarından korumak için bilgi sürekliliği faaliyetleri *Bilgi Sistemleri Süreklilik Planı* kapsamında gerçekleştirilir. Bu faaliyetlerin bilgi güvenliği gereksinimlerini karşılaması sağlanır.

4.11. 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 Şirket çalışanları, Şirket verilerinin gizlilik derecelerine uygun şekilde kullanımı konusunda sorumludurlar.

Bilgilerinize sunarız.

POFintech Ödeme Hizmetleri ve Elektronik Para Anonim Şirketi