

FINANCELL DİJİTAL GÜVENLİK

❖ BİLGİ GÜVENLİĞİ POLİTİKASI

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ VE POLİTİKALARI

Turkcell Finansman A.Ş. (Bundan böyle “Finansman Şirketi” veya “Şirket” olarak adlandırılacaktır.)’de iş ihtiyaçlarına, kanunlara ve yasal düzenlemelere uygun şekilde bilgilerin güvenliğini sağlamak amacıyla üst yönetim gözetiminde bilgi güvenliği yönetim sistemi mevcuttur. Şirket yönetimi, Finansman Şirketi’nde bilgi güvenliği yönetim sisteminin hayata geçmesi konusunda destek sağlar, gerekli durumlarda atama ve yönlendirme yapar. Bilgi güvenliği yönetim sistemi, tanımlı bir risk yönetim yaklaşımı ve temel kuralların belirlendiği bilgi güvenliği politikaları ile sağlanmaktadır. Bu politikalar, tüm Turkcell Finansman A.Ş. çalışanlarının erişebileceği şekilde şirket içerisinde paylaşılmıştır. Bilgi güvenliği politikalarının amacı, Bilgi Güvenliği risklerinin yönetilmesi ve bilginin yeterli seviyede güvenliğinin sağlanmasıdır. Tüm şirket çalışanları, sorumlusu oldukları iş süreçleri ve bilgi varlıklarında bu politikalarda yazan kuralların uygulanmasından sorumludur.

Şirketin bilgi güvenliği yönetim sisteminin uygunluğu, yeterliliği ve etkinliğinin bağımsız olarak gözden geçirilmesi sağlanır. Bağımsız gözden geçirme sonuçları, yönetime raporlanır ve ilgili kayıtlar saklanır.

GİZLİLİK ANLAŞMALARI

Her Turkcell Finansman A.Ş. çalışanının iş akdinde bilgi gizliliğini korumakla sorumlu olduğu belirtilir. Tedarikçilerle çalışmaya başlanmadan önce gizlilik anlaşması imzalanır. Şirkete devamlı ve/veya geçici olarak hizmet veren tedarikçiden alınan hizmetin/ürünün içeriği ve kapsamına göre şirketin karşılaştacağı riskler öngörülerek uygun olan güvenlik konuları gizlilik sözleşmesine eklenir. Söz konusu gizlilik sözleşmesi, bilgilerin güvenliğinin sağlanması ile ilgili gereksinimleri yansıtır ve ticari yaptırımları içerir. Korunması gereken bilgiler, ihlaller ile ilgili yaptırımlar sözleşmede tanımlanır. Tedarikçiler ve tedarikçi çalışanları görev alanları ve ilgili işteki görevleri ile sınırlı olarak bilgi varlıklarına erişmeleri gerektiği kadarıyla, minimum süreyle ve minimum erişim haklarıyla erişmeye yetkilidir.

YASAL UYUMLULUK

Şirket yasal düzenlemeler doğrultusunda güvenlik gereksinimlerini belirler ve uygular. Turkcell Finansman A.Ş. abonelerine ait tüm kişisel bilgiler, Türkiye Cumhuriyeti kanun ve düzenlemelerine uygun şekilde korunur. Kişisel bilgilerin kaydedilmesinde, işlenmesinde ve paylaşılmasında veri gizliliği ilkesine uygunluk için yürürlükteki yasa ve mevzuata uygun hareket edilir. Turkcell Finansman A.Ş. ‘nin önemli kayıtları, kayıp ve bozulmalara karşı koruma altına alınır. Kayıtların saklama süreleri belirlenirken mevzuattaki yükümlülükler dikkate alınır.

BİLGİ GÜVENLİĞİ RİSKLERİNİN YÖNETİMİ

Turkcell Finansman A.Ş. 'de bilgi güvenliği risklerinin etkin şekilde yönetilmesi için servisler ve bu servislere yönelik riskler tanımlanır. Belirlenen risklerin değerlendirilmesi ve önceliklendirilerek yönetilmesi sağlanır. Bilgi güvenliği risk yönetimi, tipik olarak risk değerlendirmeyi, risk işlemeyi, risk kabulünü ve risk iletişimini içerir.

BİLGİ GÜVENLİĞİ VAKALARININ YÖNETİMİ

Turkcell Finansman A.Ş. 'de bilgi varlıklarının güvenliğini sağlamak için teknolojik çözümler ve süreçler seviyesinde önlemler alınarak, düzenli kontrol, test ve izlemeler yapılır. Çalışanlar bu konuda bilgilendirilir ve eğitilir. Şirket bilgi varlıkları ile ilgili meydana gelen vakaların nasıl belirleneceği, kimlere iletileceği ve nasıl ele alınacağı belirlenmiştir. Ayrıca tespit edilen güvenlik zafiyetlerinin ilgililerine nasıl iletilmesi gerektiği, vakanın oluşmasına neden olan eksiklikler ve muhtemel risklerin değerlendirilmesi ile ilgili sorumluluklar tanımlanmıştır.

❖ GÜVENLİK İPUÇLARI

➤ Kişisel Bilgilerinizi ve Şifrenizi Bilgisayarınızda/Cep Telefonunuzda Saklamayın

Kimliğiniz son derece önemli bir belgedir. Bu nedenle, taranmış görüntüsünü bilgisayarınızda saklamayın.

➤ Şifrelerinizin Güvenlik Seviyelerini Yükseltin

- ✓ Financell Hesabınızda kullanıcı adı/şifre belirlerken isim, doğum tarihi gibi kolay tahmin edilebilir bilgilerden şifre belirlemeyin. Kişisel bilgilerinizi ve Financell Şifre'nizi gizli tutun, kimseyle paylaşmayın. Bu bilgileri herhangi bir yere yazmayın.

➤ Bilgilerinizi Paylaşmayın

- ✓ Financell (Turkcell Finansman A.Ş.), sözlü ya da yazılı olarak hiçbir zaman e-posta, SMS ya da telefon aracılığıyla Financell Şifre'nizi sormaz veya talep etmez. Bu nedenle sizden Financell Şifre'nizi ve talep eden 3. şahıslara şifrenizi açıklamayınız.
- ✓ Kişisel bilgilerinizi veya şifrenizi göndermenizi talep eden bir e-posta Financell'e aitmiş gibi görünen bir adresten gelirse, bu e-postaya cevap vermeyin. Financell (Turkcell Finansman A.Ş.), sözlü veya yazılı olarak hiçbir zaman e-posta, SMS ya da telefon aracılığıyla şifrelerinizi sormaz veya talep etmez.

➤ **Kişisel Bilgisayarlarınızın Güvenli Olmasına Dikkat Edin**

- ✓ Bilgisayarınızda mutlaka lisanslı programlar ve işletim sistemi kullanın. İşletim sisteminizi ve programlarınızı sürekli güncelleyin.
- ✓ Antivirüs, anti spyware ve kişisel firewall gibi koruma kalkanları kullanmaya özen gösterin.
- ✓ İnternette indirdiğiniz ya da bilgisayarınıza yüklemek istediğiniz programları mutlaka virüs taramasından geçirin. Kaynağını bilmediğiniz programları bilgisayarınıza yüklemeyin. Özellikle “.exe” uzantılı dosyalara dikkat edin.
- ✓ Uygulamalar açıkken bilgisayar başından kalkmamanızı tavsiye ederiz.

➤ **Güvenliğinden Emin Olunmayan Kablosuz Ağları Kullanmayın**

- ✓ Financell Hesabım’a internet kafe gibi halka açık veya ortak kullanımda olan bilgisayarlardan girmeyin.
- ✓ İnternet erişiminizi ADSL ile sağlıyorsanız, interneti kullanmadığınız zamanlarda bağlantınızı kapatın.
- ✓ Wi-Fi, Bluetooth, kızılötesi gibi kablosuz yöntemler cep telefonlarına yetkisiz erişim riski doğurabilmektedir. Bu nedenle güvenliğinden emin olmadığınız kablosuz ağları kullanmayınız.
- ✓ Bluetooth üzerinden gelen, kaynağını ve güvenilirliğini bilmediğiniz dosyaları da kabul etmeyin; ihtiyaç duymadığınız zamanlarda bu uygulamaları kapalı tutun.

➤ **Adres Çubuğuna www.financell.com.tr Yazarak Giriş Yapın**

- ✓ İnternet sitemizi kullanmak için herhangi bir linki tıklamak yerine www.financell.com.tr adresini tarayıcınızın adres çubuğuna yazarak giriş yapın.

❖ OLASI TEHLİKELER

İnternette güvenlik konusunda merak edilen virüs saldırıları ve benzeri diğer tehlikelere karşı önlem alabilmek için bilgi sahibi olun.

➤ Virüs Saldırıları

Bilgisayarlarınız, akıllı telefonlarınız ve tabletleriniz çeşitli yollarla virüslere maruz kalabilir:

- ✓ Sahte e-posta linkleri,
- ✓ Arama motorlarında listelenen sahte sayfa linkleri,
- ✓ İnternet sitelerindeki güvenli olmayan reklam ve sponsor linkleri
- ✓ Financell tarafından gönderiliyormuş algısı verilen SMS'ler içerisindeki linkler

➤ Phishing (Oltalama) Saldırıları

Oltalama saldırıları olarak da bilinen bu saldırı türünde genel olarak kullanıcıların **e-posta hesaplarına; yüksek fatura bilgileri, hediye, indirim, kampanya, ödül** gibi cezbedici sahte iletiler gönderilir ve **kredi kartı bilgileri, kimlik bilgisi, TCKN, müşteri numarası** gibi hassas verilerin çalınması amaçlanır. Dolandırıcılar bu bilgileri farklı amaçlar için kullanabilir. Maddi ya da manevi zarar verme amaçlanır.

Phishing (Olta) Saldırıları, çeşitli finans kurumları tarafından gönderilmiş gibi görünen, acil ve çok önemli konular içeriyormuş gibi duran sahte e-postalardır.

Oltalama Saldırılarına Karşı Alınabilecek Önlemler:

- Oltalama saldırılarından korunma yöntemlerinden en etkili; gelen eposta sizi bir siteye yönlendiriyor ise, bu sitelerin **https(s)** takılı olup olmadığını bakılır. Güvenlik sertifikası olan bir site **https** takısı alır.
- Şüpheli görülen e-postalardaki URL linkleri tıklanmaz.