GÜVENLİK VE KULLANICI BİLGİLENDİRME

TRPOS sistemleri 7/24 olmak üzere günün her saatinde bilgi sistemleri politikalarımız çerçevesinde geliştirilen ve güncellenen güvenlik önlemleri ile korunmaktadır. Ayrıca herhangi bir olağanüstü durum halinde iş sürekliliği planları ile acil ve beklenmedik durum yönetim prosedürü ile sistemin sağlıklı şekilde çalışmaya devam etmesi planlanmıştır.

Online şekilde işlem yapılan tüm ortamlar doğası gereği saldırıya açık olabilmektedir. TRPOS tarafından tüm tedbirler alınmış, acil durum planlamaları ve kriz yönetim süreçleri düzenlenmiş olsa bile kötü niyetli siber ataklar ile karşılaşılabilmesi her zaman mümkündür.

Bu çerçevede internet üzerinden işlem yapan kullanıcıların hesaplarında yetkisiz işlemlerde bulunulması, yanıltılarak kullanıcı panellerinde mevcut olmayan durumlar bilgiler var gibi gösterilmesi, dolandırıcılık ve sahtekarlığa yönelik işlemler sebebiyle zarara uğratılması, kullanılan cihazlara trojan, virüs ve benzeri kötü amaçlı yazılımların bulaştırılması ihtimal dahilindedir. Siber ataklar ile kullanıcıya ait hassas verilere ulaşılması hedeflenmektedir. Bu veriler ile kullanıcı gizli bilgileri elde edilmeye çalışılmak ta, kullanımı, manipüle edilmesi ve kamuya açıklanması söz konusu olabilmektedir. Bu sebeple kullanıcılarımız bu dökümanda ve sitede yer alan güvenlik talimatlarını uygulamaları ve hak kayıplarının engellenebilmesi veya azaltılabilmesi amacıyla TRPOS ile ivedilikle iletişime geçmeleri gerekmektedir. Güvenlik talimatlarının uygulanmaması ve TRPOS tan kaynaklanmayan durumlarda kullanıcılarımızın taleplerinin yerine getirilmemesi riski oluşacaktır.

Üye İşyeri sözleşmesi içerisinde TRPOS ile kullanıcıların karşılıklı olarak hak ve yükümlülükleri açıklanmıştır. TRPOS, tüm kullanımlar ve riskli işlemler ile ilgili hak ve yükümlülüklerin yer aldığı kullanıcı sözleşmesinin bir örneğini site üzerinde incelemeye açık tutmakta ve kullanıcıların gerekli detayda inceleme yapmalarını tavsiye etmektedir.

TRPOS ile tüm iletişimler, veriler ve web girişleri 256 bit SSL şifrelemesi ile her an koruma altında tutulmaktadır. İki faktörlü güvenlik doğrulama ile gerçek kullanıcı haricindeki kişilerin giriş yapması ve işlemlere erişmesi engellenmiştir. Bu kapsamda alınan tedbirlerin yanında, kullanıcıların doğru kanaldan TRPOS'a ulaştığından emin olması kullanıcının yararınadır. Kullanıcıların;

- Tarayıcı üzerinde giriş yapılan sistemin TRPOS sistemi olmasına, farklı sitelerden gelen linkler vasıtasıyla giriş yapılmamasına dikkat etmeleri,
- İnternet sayfası olarak https://www.trpos.com/ dan eriştiklerini ve üye işyeri sayfalarına giriş için https://merchant.trpos.com/giris olan bağlantı adresini kontrol etmeleri,
- Giriş kullanıcı adı ve şifrelerinin herhangi bir ortamda yazılı veya dijital olarak kaydedilmemesi
- Bilgilerinin TRPOS personeli dahil olmak üzere üçüncü kişilerle paylaşılmaması
- Şifre oluşturma safhasında doğum yılı, yeri gibi veya kolay tahmin edilecek kombinasyonları kullanmamaları
- Genel amaçlı kullanılan ağ ve cihazlardan bağlantı yapılmamasına özen göstermeleri

önem arz etmektedir. Bu tedbirler dolandırıcılık riskine maruz kalmamak için kullanıcı tarafından alınması gereken en önemli önlemlerdendir. TRPOS güvenlik duvarları ile korunan

bir sistem altyapısına sahiptir. Kullanıcılarımızın da bağlantı sağladıkları cihazlarda benzer şekilde güvenlik altyapısının bulunması gerekmektedir.

Kullanıcılarımız tarafından SMS iletiminde sıkıntılar yaşanması halinde sayfamızda belirtilen iletişim kanallarından bilgilendirme yapılabilmekte ve aksaklıklar hızlıca sonuçlandırılmaktadır. İletişim esnasında gelen SMS ve size özel şifreleriniz TRPOS tarafından hiçbir şekilde talep edilmemektedir. Bu şekilde gelen talepleri cevaplamamanız güvenliğinizin sağlanması için önemlidir.

TRPOS tarafından sunulan hizmetler dolayısıyla sitemizden veya mobil uygulama aracılığı ile dolandırıcılık ve sahtekarlık girişimlerine karşı güvenlik önlemlerinin azami ölçüde kullanıcı tarafından alınmış olması gerekmektedir. Bununla birlikte hizmetlerimiz dolayısıyla ödeme araçları ve hassas ödeme verilerinin kaybedilmesi, çalınması, silinmesi ya da değiştirilmesinin gerekmesi gibi durumlarda veya her türlü dolandırıcılık ve sahtekarlık şüphesi taşıyan işlemler dolayısıyla bilgi@trpos.com adresine e-posta göndererek veya +90 216 999 1830 nolu destek hattımızdan ulaşarak durumu haber verebilirsiniz.

Tüm işlemler ve talimatlar TRPOS sistemlerinde operasyon ve müşteri hizmetleri tarafından kontrol edilmekte ayrıca periyodik olarak iç kontrol faaliyetleri TRPOS bünyesinde gerçekleştirilmektedir. Ayrıca kullanıcı kayıt esnasında, gerçek ve güvenli müşteri kontrolleri yapılarak teyit işlemleri sağlandığı ölçüde kullanıcının işlem yapması sağlanmaktadır. Şüpheli girişler ve olağan olmayan kullanıcı fon hareketleri işlem bazında raporlanmakta, olağan görülmeyen hareketler onaylanmamaktadır. Ayrıca TRPOS personeli bilgi farkındalık eğitimleri ile düzenli olarak güncel sahtekârlık ve dolandırıcılık yöntemleri konusunda bilgilendirilmektedir.

TRPOS veritabanları yüksek güvenlik önlemleri ile korunmakta ve yedeklenmektedir. İşlem devamlılığının sağlanması için donanım ve yazılım destekleri eşzamanlı olarak gerçekleştirilmektedir. Veritabanları güvenliğinin sağlanması için en az iki farklı merkezde depolama yapılmaktadır.

Kullanıcı bilgilerinin güvenliği için kişisel verilerin korunması politikası oluşturularak uygulamaya alınmıştır. Bu kapsamda bilgi talepleriniz için ilgili politikaları inceleyebilir ve belirtilen kanallardan iletişime geçebilirsiniz. Sitemize farklı bağlantılardan geldiğinizde çerez verileri toplanabilmektedir. Çerez politikası içerisinde yer alan yönergeleri takip ederek çerezlerin kapatılması mümkündür.

TRPOS ÖDEME KURULUŞU A.Ş.