



BİTBNS KRİPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

**PIYASA FİYATLARINI VE PLATFORM İŞLEYİŞİNİ ETKİLEYEN DURUMLAR İLE ALINAN
ÖNLEM VE TEDBİRLERE İLİŞKİN AÇIKLAMA**

BİTBNS KRIPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

PIYASA FİYATLARINI VE PLATFORM İŞLEYİŞİNİ ETKİLEYEN DURUMLAR İLE ALINAN ÖNLEM VE TEDBİRLERE İLİŞKİN AÇIKLAMA

1. AMAÇ VE KAPSAM

İşbu Piyasa Fiyatlarını ve Platform İşleyişini Etkileyen Durumlar ile Alınan Önlem ve Tedbirlere İlişkin Açıklama, Bitbns Kripto Varlık Alım Satım Platformu Anonim Şirketi (“**Şirket**”) tarafından sunulan kripto varlık işlem platformu üzerinde (“**Platform**”) sağlanacak hizmetleri (“**Hizmet**”) kullanacak müşterilerimizin (“**Müşteri**”) piyasa fiyatlarında ani ve beklenmedik dalgalanmalara yol açabilecek ve Platform’un işleyişini etkileyebilecek durumlar hakkında bilgilendirilmesi amacıyla hazırlanmıştır.

2. PİYASA FİYATLARINI VE PLATFORM İŞLEYİŞİNİ ETKİLEYEN DURUMLAR

- 2.1.** Kripto varlık piyasalarındaki fiyatlar arz ve talep doğrultusunda belirlenmektedir ve fiyatlar serbestçe oluşmaktadır. Ancak söz konusu fiyatların oluşumu her zaman rasyonel bir gerekçeye dayanmayabilir. Bazı kripto varlıkların irrasyonel fiyat hareketleri dolayısıyla beklenmedik zararlara uğrayabilirsiniz. Belirli bir kripto varlığa olan piyasa talebinin tamamen ortadan kalkması durumunda, söz konusu kripto varlığın değerinin tamamen ve kalıcı olarak yok olma riski bulunmaktadır.
- 2.2.** Belirli piyasa koşullarında, kripto varlıkların alım ve satımı önemli derecede zorlaşabilir veya hiç mümkün olmayabilir. Özellikle, piyasada yeterli likiditenin bulunmaması, emirlerin gerçekleştirilmesini engelleyebilir ya da işlemlerin beklenenden daha büyük fiyat sapmalarıyla sonuçlanmasına neden olabilir.
- 2.3.** Kripto varlık piyasaları bazen yeterli likiditeye sahip olmayabilir, bu da alım satım işlemlerinin beklenen fiyatlarda veya hızda gerçekleşmemesine yol açabilir. Bazı kripto varlıklar (özellikle daha az bilinen veya yeni çıkanlar bunlara örnek olabilir), sınırlı seviyede alıcı ve satıcı sayısı nedeniyle düşük likiditeye sahip olabilir. Bu durum, Müşteriler’in varlıklarını istediği zaman ve fiyatta satmasını veya satın almasını zorlaştırabilir. Piyasa likiditesinin düşük olması, fiyat dalgalanmalarını daha da artırabilir ve beklenmedik kayıplara yol açabilir. Bu sebeple işlem yapılması düşünülen kripto varlıkların likidite seviyelerinin değerlendirilmesi ve likidite risklerinin dikkate alınması önemlidir.
- 2.4.** Platform’da ve/veya uygulamalarımızda işlem yapılırken sistem hataları oluşabilir. Müşteri, sistemden kaynaklı bir arıza nedeniyle emirlerinin ertelenebileceği, gecikebileceği veya geçersiz sayılabileceği riskinden haberdardır. Müşteri, internet tabanlı bir sisteminin kullanımı sırasında ortaya çıkabilecek geniş yelpazedeki birçok riskle karşılaşabileceğini göz önünde bulundurmalıdır. Bu riskler, donanımsal, yazılımsal veya internet bağlantılarındaki arızalarla ilgili olabilir. Bu bağlamda, kesinlikle sınırlayıcı olmaması kaydıyla, Müşteri farkındalığını artırmak amacıyla Müşteri’nin karşı karşıya olduğu bazı risklere örnek vermek gerekirse: kötü amaçlı yazılımların bulaşması; üçüncü tarafların Müşteri’ye ait bilgi ve dijital varlıklara yetkisiz erişimi; siber saldırılar; yapay zeka tabanlı saldırılar; sosyal mühendislik saldırıları; kripto varlık ağına ilişkin hatalar; bilgisayar virüsleri; iletişim kesintileri; sistem arızaları ve gecikmeler gibi riskler söz konusu olabilmektedir. Ayrıca, casus yazılım, truva atları, solucanlar ve kimlik avı gibi Müşteri’ye veya cihazlarına zarar verebilecek diğer kötü amaçlı yazılım tehditleri de ortaya çıkabilmektedir. Bu tür riskler gelişen teknolojiyle her geçen gün değişmekte ve farklı görünümlere bürünebilmektedir. Müşteri kullandığı donanımın, yazılımın, internet bağlantısının ve diğer çevresel elemanların risklerden arı olduğunu kontrol etmelidir.

- 2.5. Platform'a, müşteri hesaplarına ve bu hesaplarda tutulan kripto varlıklara yönelik saldırılar gerçekleşebilir.
- 2.6. Bazı kripto varlıkların işlem gördüğü ağın son bulması, geliştiricilerinin projeden çekilmesi, onaylayıcıların ağdan çekilmesi, kripto varlıkların değer kaybetmesi, kripto varlıkların veya bunlara bağlı olarak yapılan işlemlerin devlet tarafından veya herhangi bir resmi, idari otorite veya yasal merciler tarafından yasaklanması, tedbir uygulanması, engellenmesi gibi riskler bulunmaktadır.

3. ÖNLEM VE TEDBİRLER

- 3.1. Müşteri, hesabının güvenliğinden sorumlu olup; Müşteri hesabına erişim için kullandığı şifre ve/veya diğer bilgileri güvenli bir şekilde korumak zorundadır. Ayrıca Müşteri, hesabının durumunu her zaman takip etmelidir.
- 3.2. Kripto varlıkların çoğunluğu, çevrimdışı olan ve çevrimiçi tehditlerden korunan soğuk cüzdanlarda saklanmaktadır. Operasyonel ihtiyaçlar için, kullanılan sıcak cüzdanlar çok faktörlü kimlik doğrulama, şifreleme ve gerçek zamanlı izleme ile korunmaktadır. Bu sayede risk en aza indirilerek Müşteri varlıkları güvence altına alınmaktadır.
- 3.3. Şirket, güvenlik stratejileri çerçevesinde sektör standartlarını uygulamaktadır. Çoklu imza cüzdanları kullanılmakta ve özel anahtar yönetimi sistemi, güvenli anahtar üretimi, saklama ve yönetim için donanım güvenlik modülleri dahil olmak üzere en iyi uygulamaları takip etmektedir.
- 3.4. Kripto varlıklarla ilgili tüm hassas veriler hem saklama hem de aktarım sırasında sektör standartlarında şifreleme protokolleri kullanılarak şifrelenir. Kritik sistem ve verilere yalnızca yetkili personelin erişebilmesini sağlamak için sıkı erişim kontrol politikaları uygulanmaktadır. Gerçek zamanlı izleme ve uyarı sistemleri devreye alınmıştır.
- 3.5. Güvenlik kontrollerinin etkinliğini değerlendirmek ve iyileştirilmesi gereken alanları belirlemek için düzenli güvenlik denetimleri yapılmaktadır.
- 3.6. Müşterilerin Platform güncellemelerini ve güvenlik duyurularını düzenli olarak takip etmeleri, herhangi bir güvenlik ihlali durumunda hızlı hareket edebilmeleri için önemlidir. Teknolojik yenilikler ve güncellemeler, kripto varlık işlemlerinin güvenliğini ve işlevselliğini etkileyebilir, bu nedenle sürekli bilgi güncellemesi yapmak ve sahip olunan donanımların/yazılımların ve aygıtların güncel tutulmasını sağlamak esastır.
- 3.7. Kullanıcılar tarafından phishing (oltalama) saldırılarına karşı dikkatli olunmalı ve herhangi bir şüpheli aktivite derhal Platform'a bildirilmelidir. Kullanıcıların, cihaz güvenliği için güncel ve lisanslı antivirüs yazılımlarını kullanmaları ve güvenli olmayan ağ bağlantılarından kaçınmaları önerilir.