



BİTBNS KRİPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

**ACİL DURUM İLETİŞİM BİLGİLERİ VE RİSKİN AZALTILMASINA YÖNELİK
TEDBİRLERE İLİŞKİN AÇIKLAMA**

BİTBNS KRIPTO VARLIK ALIM SATIM PLATFORMU ANONİM ŞİRKETİ

ACİL DURUM İLETİŞİM BİLGİLERİ VE RİSKİN AZALTIILMASINA YÖNELİK TEDBİRLERE İLİŞKİN AÇIKLAMA

1. AMAÇ VE KAPSAM

Bitbns Kripto Varlık Alım Satım Platformu Anonim Şirketi (“**Şirket**”), kripto varlıklara ve işlemlere yönelik olası riskler hakkında müşterilerini bilgilendirmiştir. İşbu Acil Durum İletişim Bilgileri ve Riskin Azaltılmasına Yönelik Tedbirlere İlişkin Açıklama (“**Açıklama**”), beklenmedik durum planlarına uygun olarak, olası risklerin gerçekleşmesi halinde müşteri mağduriyetini asgari seviyeye indirebilmek için alınan tedbirler ile, acil durumlarda kullanılacak iletişim bilgilerini içermektedir.

Bu Açıklama; başta bilgi teknolojileri riskleri olmak üzere Şirket’i etkileyebilecek riskleri dikkate alarak, risk yönetimine dair alınabilecek önlemler hususunda bütüncül bir yaklaşım benimsemektedir. Bu risklerin etkin bir şekilde önlenmesi için, Şirket’in risk yönetimi uygulamalarının temelini oluşturan üst düzey aksiyonlar ve alınması gereken asgari tedbirler açıklanmaktadır.

Bu Açıklama yılda en az 1 defa gözden geçirilir. İç kontrol birimi, işbu Açıklama’da yapılacak önemli değişiklikleri denetlemek, gözden geçirmek ve onaylamaktan sorumludur.

İlgili mevzuatın çeşitli maddeleri ilerleyen tarihlerde yürürlüğe girecektir ve bu Açıklama’daki yükümlülükler ilgili mevzuat hükümleri yürürlüğe girdiği tarihten itibaren uygulanır.

2. RİSKLER VE ALINACAK TEDBİRLER

2.1. Tanım

Şirket’i etkileyebilecek riskler risk yönetimine ilişkin politika ve prosedürlerde ve risk matrislerinde kategorize edilmiş ve tanımlanmıştır.

Bilgi teknolojileri riskleri, Şirket’in teknolojik sorunlar, sistem sorunları veya siber saldırılar nedeniyle karşılaştığı potansiyel tehditleri, veri kayıp ve ihlallerini ve güvenlik açıklıklarından kaynaklanan riskleri ifade etmektedir.

2.2. Şirket Tarafından Alınacak Tedbirler

Etkin risk yönetimi Şirket operasyonlarının temel taşıdır. Müşteri varlıklarının ve operasyonların güvenliğini sağlayarak Şirket’i etkileyebilecek riskleri belirlemek, değerlendirmek ve azaltmak için kapsamlı süreçler oluşturulmuştur.

Şirket’in risk yönetimi süreci aşağıdaki adımlardan oluşmaktadır:

- (a) Risk tanımlama,
- (b) Risk değerlendirmesi,
- (c) Risk azaltma,
- (d) Risk izleme,
- (e) Risk raporlama
- (f) Sürekli iyileştirme.

Şirket siber güvenlik risklerini azaltmak için müşteri varlıklarını sigortalamakta, çok faktörlü kimlik doğrulama yöntemleri uygulamakta, güvenlik açıklarını belirlemek için düzenli penetrasyon testleri yapmakta ve diğer gerekli tedbirleri almaktadır.

2.3. Müşteriler Tarafından Alınacak Tedbirler

Müşteri hesabı ve varlıklarına ilişkin oluşan risklerin önlenmesi ve giderilmesi için, Şirket müşterilerine aşağıda örnek olarak sıralanan tedbirleri almaları tavsiye edilmektedir:

- (a) İki Faktörlü Kimlik Doğrulama (2FA) etkinleştirilmelidir.
- (b) Şifreler karmaşık ve tahmin edilemez olmalı; aynı şifre başka yerlerde kullanılmamalı ve düzenli olarak değiştirilmelidir.
- (c) Bilinmeyen kaynaklardan gelen bağlantılara tıklanmamalı, e-postalar dikkatle incelenmelidir.
- (d) E-posta hesabı güvenliği sağlanmalıdır.
- (e) Giriş yapılan cihazların antivirüs yazılımı ve güncellemeleri tam olmalıdır.
- (f) Düzenli olarak işlem sonuç formları ve hesap ekstreleri kontrol edilmelidir.
- (g) Giriş bilgilerinin ve 2FA anahtarlarının yedekleri güvenli şekilde saklanmalıdır.
- (h) Hesaba erişim kaybı durumunda, kimlik doğrulama süreci bilinmelidir.
- (i) Şüpheli hareketlerde, Şirket'in müşteri Şikayet ve İtiraz Yönetimi Prosedürü'nden yararlanılmalıdır ve söz konusu prosedürde belirtilen iletişim kanallarından veya aşağıda belirtilen acil durum iletişim bilgileri üzerinden, Şirket personeli ile derhal iletişime geçilmelidir.

3. ACİL DURUM İLETİŞİM BİLGİLERİ

3.1. Acil Durum Örnekleri

Örnek olarak sayılan ve aşağıda belirtilen acil durumlardan birinin gerçekleşmesi halinde, müşteriler; Şirket tarafından sunulan hizmetlere ilişkin olarak aşağıdaki iletişim adresleri yoluyla ilgili Şirket personeli ile iletişime geçebilirler:

- (a) Hesabın hacklenmesi (şifrenin ele geçirilmesi, yetkisiz giriş),
- (b) Kimlik avı (phishing) saldırıları sonucu giriş bilgilerinin çalınması,
- (c) Bakiye görüntüleme sorunları (varlıkların görünmemesi veya hatalı gösterimi),
- (d) Cüzdan işlemlerindeki gecikmeler (çekim veya yatırma işlemlerinin uzaması),
- (e) API kesintileri,
- (f) Platformun saldırıya uğraması (örneğin: DDoS saldırıları),
- (g) Müşterinin hesabına erişememesi (şifre unutma, e-posta kaybı),
- (h) Kripto varlık kayıpları yaşanması (personel hatası, teknik arıza vb. nedenleriyle),
- (i) Mobil uygulama veya internet sitesine erişim kesintisi.

3.2. Acil Durum İletişim Bilgileri

Acil durumların gerçekleşmesi halinde, müşterilerin irtibata geçebileceği Şirket biriminin iletişim bilgileri aşağıdadır:

Görevli Birim : Bilgi Teknolojileri Birimi

Adres : Barbaros Mah. Ak Zambak Sok. Uphill Towers Sitesi No: 3A
İç Kapı No:35 Ataşehir / İstanbul

E-posta Adresi : destek@bitbns.com