1. **Amaç ve Kapsam**

Bu Kurtarma Planı Prosedürü, kripto varlık kaybı sonucunu doğurabilecek eylem ve risklerin tespit edilerek, bu risk ve eylemlerin gerçekleşmesi durumunda alınacak aksiyonların belirlenmesi amacıyla oluşturulmuştur.

2. Dayanak

Bu Prosedür aşağıda sayılan Kanun ve düzenlemeleri başta olmak üzere kripto varlık hizmet sağlayıcıların tabi olduğu mevzuat temel alınarak hazırlanmıştır.

- 6362 sayılı Sermaye Piyasası Kanunu,
- III-35/B.1 Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ
- III-35/B.2 Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları ile Sermaye Yeterliliği Hakkında Tebliğ

3. Tanımlar

3.1. Platform: Crybo Kripto Varlık Alım Satım Platformu A.Ş.'yi

3.3. Cüzdan: Kripto varlıkların transfer edilebilmesini ve bu varlıkların ya da bu varlıklara ilişkin özel ve açık anahtarların depolanmasını sağlayan yazılım, donanım, sistem ya da uygulamaları,

3.4. Kripto varlık: Dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıkları,

3.5. Kurul: Sermaye Piyasası Kurulu'nu,

3.6. MASAK mevzuatı: 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun ve ilgili alt düzenlemeleri,

3.7. Mevzuat: 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununu, III-35/B.1 Kripto Varlık Hizmet Sağlayıcıların Kuruluş ve Faaliyet Esasları Hakkında Tebliğ, III-35/B.2 Kripto Varlık Hizmet Sağlayıcıların Çalışma Usul ve Esasları ile Sermaye Yeterliliği Hakkında Tebliği, İlke Kararları ve diğer ilgili düzenlemeleri,

3.8. Sıcak cüzdan: Kripto varlık hizmet sağlayıcıların müşterilerinin kripto varlık transferlerini karşılamak için kullandıkları, internete bağlı olan ve soğuk cüzdan özelliği göstermeyen cüzdan teknolojisini,

3.9. Soğuk cüzdan: Kripto varlığın kontrolünü sağlayan anahtarların fiziksel, idari ve teknik bilgi güvenliği kontrolleri ile korunduğu, işlem onaylama ve işlem imzalama gibi kritik işlemlerin buna yetkili personel müdahalesiyle fiziki veya teknik hava boşlukları ile internetten izole edilmiş ortamlarda yapılmasına olanak sağlayan cüzdan teknolojisini

3.10. Kripto Varlık Transferi: Cüzdanlarda bulunan kripto varlıkların dağıtık defter teknolojisi üzerinden başka cüzdanlara aktarımını,

ifade eder.

4. Öngörülen Riskler

Kripto varlık kaybı sonucu doğabilecek riskler tanımlanırken Platformun tüm güvenlik unsurları dikkate alınır. Asgari olarak bilişim sistemlerinin işletilmesinden, bilişim sistemlerine yapılabilecek yetkisiz değişikliklerden, varlıkların yetkisiz kişilerin eline geçmesinden, saldırı sonucu kullanıcıların sisteme erişememesinden, fiziksel güvenlikten, her türlü siber saldırıdan, bilgi güvenliği ihlallerinden, personelin dış kaynaklı zorlama ve benzeri nedenlerle yasal olmayan faaliyetlerde bulunmasından veya personelin davranışından kaynaklanabilecek riskler göz önünde bulundurulur.

4.1. **Operasyonel Risk:** İçsel süreçlerin, insanların, sistemlerin ya da harici olayların neden olduğu ve yasal riski de kapsayan zarar olasılığını ifade eder.

Platform mevzuat gereği ve etkin iç kontrol mekanizmalarının oluşturulması amacıyla gerekli prosedür ve dokümanları hazırlamıştır. Platformun operasyonel risk iştahı ve limitleri belirlenmiş olup, bu hususlar düzenli olarak takip edilmekte ve gerekli görüldüğü hallerde güncellenmektedir.

Operasyonel risklere yönelik olarak Platformdaki birimlerin farkındalık kazanması amacıyla gerekli bilgilendirmeler ve eğitimler sağlanmaktadır. Platform çalışanlarının kendi görev alanları dahilinde riskleri bilmesi, tespit etmesi ve gerektiğinde ilgili birime raporlama yapması beklenmektedir.

4.2. **Siber Güvenlik Riski**: Platforma siber saldırı düzenlenmesi, Kripto varlıklara yönelik olarak çalınma, çeşitli güvenlik ihlallerinin yaşanması, elektronik veya teknolojik arızalar yaşanması ve neticesinde ortaya çıkabilecek zararı ifade etmektedir.

Kripto varlıklar dijital ortamda üretilmekte, işlem görmekte, transfer edilmektedir. Bu sebeple varlık ağ hatası, bilgisayar virüsleri, iletişim hataları, aksamalar, hatalar, bozulmalar, gecikmeler, casus yazılım, scareware, truva atları, solucanlar veya bilgisayarı veya diğer ekipmanları veya olabilecek kimlik avı, casusluk veya diğer saldırıları etkileyebilecek diğer kötü amaçlı yazılımlara maruz kalabilmektedir.

Platform, bilgi sistemlerini, varlıklarını, müşteri verilerini siber tehditlere karşı korumak için gelişmiş güvenlik önlemleri almaktadır. Platform tarafından bu doğrultuda güvenlik ilkeleri benimsenmiş ve gelişime açık bir strateji planı oluşturulmuştur. Oluşturulan güvenlik strateji planı çerçevesine güncel tehditlere karşı koruma sağlamak için son teknoloji ürünü araçlar ve teknolojiler kullanılmaktadır. Bilgi sistemleri altyapısının korunması yaşanabilecek siber saldırıları ve güvenlik açıkları, tehditleri tespit etmek, hızlı bir şekilde gidermek için gerekli süreçler işletilmektedir.

4.3. **Kripto Varlık Riski**: Piyasaya erişimin kısıtlanması, network programının son bulması, geliştiricilerin projeden çekilmesi, kripto varlıkların değer kaybetmesi risklerini ifade etmektedir.

Kripto varlıkların değeri fiyatlar arz ve talep doğrultusunda belirlenmektedir Kripto Varlık piyasalarındaki değerler aşırı değişkendir. Bu sebeple mali değeri hızlıca değişebilmektedir. Platform ve Platform müşterileri, bu ani ve olumsuz değişikliklerden etkilenebilme ihtimalini barındırmaktadır.

Platform kripto varlık riskini en aza indirmek için mevzuat çerçevesinde gerekli önlemleri almaktadır.

4.3.1. **Likidite Riski:** Kripto varlıklar değişken likidite seviyelerine sahiptir. Bazı kripto varlıkların oldukça likit olmasına karşın bazılarında işlem hacmi daha düşüktür. Likiditesi düşük olan piyasalar dalgalanmayı artırabilir.

Likidite riskini en aza indirebilmek, piyasa koşullarından veya Platformun mali yapısından kaynaklanabilecek olası likidite sıkışıklıklarına karşı gerekli tedbirlerin zamanında ve doğru şekilde alınmasını sağlamak amacıyla gerekli prosedürler oluşturulmaktadır.

Piyasa fiyatlarında ani ve beklenmedik dalgalanmalara yol açabilecek; ekonomik, siyasi, teknolojik veya sistemik olaylar ile piyasada likidite eksikliğinin meydana gelmesi, ticaretin durdurulması, platformların işleyişini etkileyen teknik arızalar, siber saldırılar veya doğal afetler gibi olağan dışı durumların oluşması halinde, bunlara ilişkin kurtarma planı oluşturulmuştur.

5. Kurtarma Planı Süreci

5.1. Sıcak cüzdanlarda bulunan kripto varlıkların ivedi şekilde soğuk cüzdanlara çekilmesi

Platformda listelenen kripto varlıklar Listeleme Prosedürü ve mevzuat uyarınca soğuk cüzdanlarda saklanabilir özellikte olur. Bu Prosedür'de anılan ancak bunlarla sınırlı olmamak üzere kripto varlık kaybına yol açabilecek risklerin meydana gelmesi halinde; operasyonel süreçler kapsamında mevzuata uygun olarak sıcak cüzdanlarda bulunan kripto varlıklar gerekli cüzdan erişim prosedürleri işletilerek en kısa sürede soğuk cüzdanlara çekilir. Bu halde Yönetim Kurulu onayı gerekmektedir.

5.2. Tehdit altındaki veya olay sebebiyle etkilenen sistem ve cüzdanların diğer sistem ve cüzdanlardan izole edilmesi

Sistem ve cüzdanlar, gerekmesi halinde ayrılabilir ve tehdit altındaki ortamdan arındırılabilir şekilde belirlenmiştir. Bu kapsamda kripto varlık kaybını doğurabilecek risklerin meydana gelmesi veya tehdit unsurlarının oluşması halinde etkilenen sistem ve cüzdanlar diğer sistem ve cüzdanlarda ayrıştırılır. Operasyonel süreçlerin güvenliği için yedek sistemler devreye alınır ve kripto varlıklar cüzdan erişim prosedürleri işlenerek güvenli cüzdanlara çekilir.

5.3. Karşılaşılan durumun, etkilenen sistem, cüzdan ve olay sebebiyle oluşabilecek sistemsel zayıflıklar bakımından değerlendirilmesi

Kripto varlık kaybına neden olan veya olabilecek durumun meydana gelmesi halinde derhal etki değerlendirme süreci işletilir. Kurtarma planının uygulamaya konulması durumunda risk yönetim birimi tarafından planın iş akış prosedürlerine uygun olarak yürütülüp yürütülmediğine ve karşılaşılan durumun müşteri varlıklarına ve Platforma olası mali etkisine ilişkin bir değerlendirme raporu hazırlanır ve yönetim kuruluna sunulur. Biri en az genel müdür yardımcısı düzeyinde olmak üzere iki personel kurtarma planının uygulanmasından sorumlu kişiler olarak yönetim kurulunca belirlenmiştir.

Platform tarafından kurtarma planlarının uygulanacak durumda olması halinde kurtarma planlarının nasıl uygulanacağı ve buna ilişkin iş akış prosedürleri hakkında müşterilere internet sitesi aracılığıyla bilgi verilir.

5.4. Mevzuat uyarınca tutulması gereken tüm belge ve kayıtların tutulmaya devam edilmesinin sağlanması

Platformun ikincil sistemleri birincil sistemle aynı risklere maruz kalmayacak şekilde belirlenmiştir. Platformun tutmakla yükümlü olduğu belge ve kayıtların yedekleri belirli aralıklarla alınır ve muhafaza edilir. Mevzuat ve MASAK mevzuatı uyarınca tutulması gereken tüm kayıt ve belgelerin güvenliği sağlanır ve bilgi, belge ve veri kaybı önlenir.

5.5. Tehdidin ortadan nasıl kaldırılabileceği ve sistem ile cüzdan güvenliğinin tekrar nasıl sağlanacağı süreçleri

Platformun kripto varlık, bilgi varlıkları ve sistemlerine ilişkin olarak kayıp tehdidi ile karşılaşması halinde derhal aksiyon alınır. Potansiyel etki analizi, olasılık değerlendirmesi ve risk önceliklendirmesi yapılır.

DERECELENDİRME	ETKİ
Hafif	Platformun işleyişini ve operasyonlarının sürekliliğini etkileme ihtimali bulunmamaktadır. Herhangi bir finansal kayıp veya veri kaybı riski bulunmamaktadır.
Orta	Plaformun işleyişinin kısa süreli askıya alınma olasılığı vardır. Kişisel veri ve gizli bilgi ihlali, bilgi bütünlüğünün bozulma olasılığı vardır ve erişilebilirlik ortaya çıkabilir. Finansal kayıp söz konusu olabilir.
Ciddi	Plaformun işleyişinin uzun süreli askıya alınır ve finansal kaybı oluşur.
Çok Ciddi	Platformun sistem erişiminin tamamen veya kabul edilemez bir süre durması söz konusu olur. Bilgi bütünlüğü geri dönülemez şekilde bozulur. Veri ve gizli bilgi kaybı veya geri dönülemez bir şekilde imhası söz konusu olur. Çok önemli finansal kayıp ortaya çıkar.

Biri en az genel müdür yardımcısı düzeyinde olmak üzere iki personel kurtarma planının uygulanmasından sorumlu kişiler olarak yönetim kurulunca belirlenmiştir. Bu kişiler bilgi güvenliği sorumlusu ile birlikte aksiyon planı belirler.

MÜDAHALE SÜRESİ	DETAY
Acil	Seviyesi çok ciddi olarak değerlendirilen risklerin oluşması veya meydana gelmesi halinde derhal aksiyon alınır.
Günlük	Seviyesi ciddi olarak değerlendirilen risklerin oluşması veya meydana gelmesi halinde bir iş günü içerisinde aksiyon alınır
3 Gün	Seviyesi orta olarak değerlendirilen risklerin oluşması veya meydana gelmesi halinde azami 3 iş günü içerisinde aksiyon alınır.
Haftalık	Seviyesi düşük olarak değerlendirilen risklerin oluşması veya meydana gelmesi halinde 5 iş günü içerisinde aksiyon alınır.

5.6. Tehdidin veya olaya sebep olan zayıflığın kaynağının tespit edilmesinde kullanılabilecek araç ve yöntemler

Tehdidin oluşması veya gerçekleşen riskin ortadan kaldırılması akabinde tehdide veya olaya sebep olan zayıflık unsurunun tespitine yönelik çalışma yapılır.

Bu kapsamda Platformun sistemlerine yönelik raporlamalar geriye yönelik olarak incelenir. Platformun tüm birimleri ortak çalışma yürüterek zayıflık unsurunun ortadan kaldırılmasını sağlar.

Platform tespit edilen risklere ilişkin olarak müdahale planları hazırlar ve hazırlanan müdahale planları yılda bir kez test edinilerek test sonuçları yönetim kuruluna raporlanır.

5.7. Faaliyete devam edilemeyeceği yönünde karar verilmesi durumunda müşterilere ait kripto varlıkların transferi

Bu halde Platform detaylı bir değerlendirme yapar. Müşterilere ait kripto varlıkların transferi için tüm müşteriler ile yazılı veya yazılı şekil yerine geçecek şekilde elektronik ortamda mutabakat yapılır. Müşteri menfaatleri ön planda tutularak müşterilere ait kripto varlıkların transferi gerçekleştirilir.

6. Bildirim

Platform tarafından kurtarma planlarının uygulanacak durumda olması halinde kurtarma planlarının nasıl uygulanacağı ve buna ilişkin iş akış prosedürleri hakkında müşterilere internet sitesi aracılığıyla bilgi verilir. Ayrıca bu halde ve Platformun operasyonel süreçlerinin etkilenmesi durumunda Kurul derhal alınan önlemler hakkında yazılı ve elektronik olarak bilgilendirilir. Bu kapsamda etki analiz raporları, alınan ve alınması planlanan önlemler ve sürece ilişkin plan Kurul'a bildirilir.

7. Gözden Geçirilmesi ve Yürürlük

Bu Prosedür yılda en az bir defa Kurul tarafından yapılan mevzuat değişikliklerinin işlenmesi ve uygulamada kazanılan deneyimler dikkate alınarak gözden geçirilir ve prosedürde gerekli güncellemeler yapılır. Bu Prosedürün yeterliliğinin yıllık olarak veya yönetim kurulu tarafından gerekli olduğunun takdir edilmesi halinde yıl periyodu beklenmeksizin gözden geçirilir ve gerekli değişiklikler yapılır.