Kurtarma Planı Prosedürü

Versiyon No	Versiyon Tarihi
1.0	25.03.2025

Recovery Plan Procedure

Version No	Date of Version
1.0	25.03.2025

1. **Prosedür Hakkında**

Fuze Kripto Varlık Alım Satım Platformu A.Ş. tarafından, tabi olunan mevzuat kapsamında bu Kurtarma Planı Prosedürü hazırlanmıştır. Platform, yürürlükteki tüm düzenlemelere uyumu sağlamak için etkili sistemler oluşturmaya ve uygulamaya kararlıdır.

Bu Prosedür'ün amacı; kripto varlık kaybı sonucunu doğurabilecek eylem ve risklerin tespit edilerek, bu risk ve eylemlerin gerçekleşmesi durumunda alınacak aksiyonların belirlenmesidir.

Bu Prosedür ile yürürlükteki mevzuata ve sektördeki en iyi uygulamalara uyum sağlanması amaçlanmaktadır.

2. **Tanımlar**

Platform: Fuze Kripto Varlık Alım Satım Platformu A.Ş.'yi,
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,
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,
Kurul: Sermaye Piyasası Kurulu'nu,
Mevzuat: 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanununu, III-35/B.1 Kripto Varlık Hizmet

1. **About the Procedure**

Fuze Kripto Varlık Alım Satım Platformu A.Ş. has prepared this Recovery Plan Procedure in accordance with the applicable legislation. The Platform is committed to creating and implementing effective systems to ensure compliance with all applicable regulations.

The purpose of this Procedure is to determine the actions and risks that may result in the loss of crypto assets and to determine the actions to be taken in case these risks and actions are realised.

With this Procedure, it is aimed to comply with the legislation in force and the best practices in the sector.

2. **Definitions**

Definitions shall mean the following:

Platform: Fuze Kripto Varlık Alım Satım Platformu A.Ş.,

Wallet: Software, hardware, systems or applications that enable the transfer of crypto assets and the storage of these assets or private and public keys related to these assets,

Crypto asset: Intangible assets that can be created and stored electronically using distributed ledger technology or similar technology, distributed over digital networks, and can express value or rights,

The Board: The Capital Markets Board,

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 düzenlemeler,

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

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

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,

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

ifade eder.

3. **Genel Esaslar**

3.1. Platform kripto varlık kaybı sonucunu doğurabilecek eylem ve riskleri tespit ederek gerekli tedbirleri belirlemekte ve bu risklerin gerçekleşmesi halinde alınacak aksiyonların çerçevesini oluşturmaktadır.

Kripto varlık kaybı sonucunu doğurabilecek riskler tanımlanırken Platform'un 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.

Legislation: Capital Markets Law dated 6/12/2012 and numbered 6362, III-35/B.1 Communiqué on Establishment and Operating Principles of Crypto Asset Service Providers, III-35/B.2 Communiqué on Operating Procedures and Principles and Capital Adequacy of Crypto Asset Service Providers, Principle Decisions and other relevant regulations

MASAK legislation: Law No. 5549 on Prevention of Laundering Proceeds of Crime and related sub-regulations,

Hot wallet: The wallet technology that crypto asset service providers use to meet the crypto asset transfers of their customers, which is connected to the internet and does not show cold wallet features,

Cold wallet: Wallet technology where the keys that provide the control of the crypto asset are protected by physical, administrative and technical information security controls, allowing critical transactions such as transaction confirmation and transaction signing to be performed in environments isolated from the internet by physical or technical air gaps with the intervention of authorised personnel,

Crypto Asset Transfer: Transfer of crypto assets in wallets to other wallets via distributed ledger technology.

3. **General Principles**

3.1. The platform identifies actions and risks that may result in loss of crypto assets, determines the necessary measures and establishes the framework of actions to be taken in case these risks are realised.

All security elements of the Platform are taken into consideration when defining the risks that may result in crypto asset loss. As a minimum, the risks that may arise from the operation of information systems, unauthorised changes to information systems, unauthorised access of assets to unauthorised persons, inability of users to access the system as a

Kripto varlıklar kaybı sonucunu doğurabilecek riskler şu şekilde belirlenmiştir:

- **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 Platformteki 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.

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

Kripto Varlıklar'ın 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.

- **Siber Güvenlik Riski**: Platform'a siber saldırı düzenlenmesi, Kripto Varlıklar'a 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,

result of an attack, physical security, all kinds of cyber-attacks, information security breaches, illegal activities of personnel due to external coercion and similar reasons, or the behaviour of personnel are taken into consideration.

The risks that may result in the loss of crypto assets are determined as follows:

- **Operational Risk:** It refers to the possibility of loss caused by internal processes, people, systems or external events, including legal risk.

The Platform has prepared the necessary procedures and documents in accordance with the legislation and in order to establish effective internal control mechanisms. The operational risk appetite and limits of the Platform have been determined, and these issues are regularly monitored and updated when deemed necessary.

Necessary information and trainings are provided to raise awareness of the units in the Platform regarding operational risks. Platform employees are expected to know and identify risks within their areas of responsibility and report to the relevant unit when necessary.

- **Crypto Asset Risk:** It refers to the risks of restriction of access to the market, termination of the network programme, withdrawal of developers from the project, depreciation of crypto assets.

The value of Crypto Assets is determined by prices in line with supply and demand. Values in Crypto Asset markets are extremely volatile. For this reason, the financial value can change rapidly. The Platform and Platform customers may be affected by these sudden and unfavourable changes.

The Platform takes the necessary measures within the framework of the legislation to minimise the risk of Crypto Assets.

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.

- **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 Platform'un mali yapısından kaynaklanabilecek olası likidite sıkışıklıklarına karşı gerekli tedbirlerin zamanında ve doğru şekilde alınmasını sağlamak amacıyla gerekli prosedürler oluşturulmaktadır.

3.2. 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.

4. **Kurtarma Planı**

- **Cyber Security Risk:** It refers to cyber-attacks on the Platform, theft of Crypto Assets, various security breaches, electronic or technological malfunctions and the damage that may arise as a result.

Crypto Assets are produced, traded and transferred in digital environment. For this reason, the asset may be exposed to network failure, computer viruses, communication errors, disruptions, failures, errors, corruptions, delays, spyware, scareware, trojans, worms or other malware that may affect the computer or other equipment or possible phishing, espionage or other attacks.
The Platform takes advanced security measures to protect its information systems, assets and customer data against cyber threats. In this direction, security principles have been adopted by the Platform and a strategy plan open to development has been established. State-of-the-art tools and technologies are used to protect against current threats within the framework of the security strategy plan.

Necessary processes are carried out to detect and quickly eliminate cyber-attacks and security vulnerabilities and threats that may occur to protect the information systems infrastructure.

- **Liquidity Risk:** Crypto assets have variable liquidity levels. While some crypto assets are highly liquid, some have lower transaction volumes. Markets with low liquidity may increase volatility.

Necessary procedures are established in order to minimise liquidity risk and to ensure that necessary measures are taken in a timely and correct manner against possible liquidity shortages that may arise from market conditions or the Platform's financial structure.

3.2. In the event of economic, political, technological or systemic events that may cause sudden and unexpected fluctuations in market prices, and in

4.1. **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.

4.2. **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.

4.3. **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

the event of extraordinary situations such as lack of liquidity in the market, trading suspension, technical failures affecting the functioning of platforms, cyber attacks or natural disasters, a recovery plan has been established.

4. **Recovery Plan**

4.1. **Immediate withdrawal of crypto assets in hot wallets to cold wallets**

Crypto assets listed on the platform can be stored in cold wallets in accordance with the Listing Procedure and legislation. In the event of risks that may lead to loss of crypto assets, including but not limited to the risks mentioned in this Procedure, crypto assets in hot wallets in accordance with the legislation within the scope of operational processes are withdrawn to cold wallets as soon as possible by operating the necessary wallet access procedures.

In this case, the approval of the Board of Directors is required.

4.2. **Isolating systems and wallets under threat or affected by the incident from other systems and wallets**

Systems and wallets are determined in such a way that they can be separated and purified from the threatened environment if necessary.

In this context, in the event that risks that may lead to loss of crypto assets occur or threat elements occur, the affected systems and wallets are separated from other systems and wallets. Backup systems are activated for the security of operational processes and crypto assets are withdrawn to secure wallets by processing wallet access procedures.

4.3. **Assessment of the situation encountered in terms of the affected system, wallet and system vulnerabilities that may be caused by the incident**

varlıklarına ve Platform'e 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.

ETKİ TABLOSU		
DERECELENDİRME		**ETKİ**
1	**ÇOK HAFİF**	Platform'un işleyişini ve operasyonlarının sürekliliğini etkileme ihtimali bulunmamaktadır.
2	**HAFİF**	Platform'un operasyonlarının sürekliliği ve güvenliğinin kısa süreli sekteye uğrayabilme ihtimali vardır. Platform sistemleri geri döndürülebilecek şekilde kısa süreli etkilenebilir.
3	**ORTA**	Plaformun işleyişinin kısa süreli askıya alınma olasılığı vardır. Kişisel veri ve gizli bilgi ihlali, bilgi bütünlüğünün bozulma olasılığı vardır ve erişilebilirlik ortaya çıkabilir. Mali kayıp söz konusu olabilir.
4	**CİDDİ**	Plaformun işleyişinin uzun süreli askıya alınır ve mali kaybın oluşur.
5	**ÇOK CİDDİ**	Platformun sistem erişiminin tamamen veya kabul edilemez bir süre durması söz konusu olur. Bilgi bütünlüğü geri dönülemez şekilde bozulur. Kişisel veri ve gizli bilgi imhası veya geri dönülemez bir şekilde imhası söz konusu olur. Çok önemli mali kayıp ortaya çıkar.

In the event of a situation that causes or may cause loss of crypto assets, the impact assessment process is carried out immediately.

In the event that the recovery plan is put into practice, an assessment report is prepared by the risk management unit on whether the plan is carried out in accordance with the workflow procedures and the possible financial impact of the situation encountered on customer assets and the Platform and submitted to the board of directors.

Two personnel, one of whom is at least at the level of assistant general manager, have been designated by the board of directors as the persons responsible for the implementation of the recovery plan.

IMPACT TABLE		
RATING		**IMPACT**
1	**VERY LIGHT**	It is not likely to affect the functioning of the Platform and the continuity of its operations.
2	**LIGHT**	There is a possibility of short-term disruption to the continuity and safety of the platform's operations. Platform systems may be irreversibly affected for a short period of time.
3	**MEDIUM**	There is a possibility of short-term suspension of the functioning of the platform. There is a possibility of personal data and confidential information breach, disruption of information integrity and accessibility. There may be financial loss.
4	**SERIOUS**	Prolonged suspension of the functioning of the platform and financial loss occurs.

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.

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

Platformun ikincil sistemleri birincil sistemle aynı risklere maruz kalmayacak şekilde seçilmiştir.

Platform'un tutmakla yükümlü olduğu belge ve kayıtların yedekleri belirli aralıklarla alınır.

Bu kapsamda mevzuat ve MASAK mevzuatı uyarınca tutulması gereken tüm kayıt ve belgelerin güvenliği sağlanır ve bilgi, belge ve veri kaybı önlenir.

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

Platform'un kripto varlık, bilgi varlıkları ve sistemlerine ilişkin olarak kayıp tehdidi ile karşılaşması halinde derhal aksiyon alınır.

Bu çerçevede öncelikli olarak tehdit belirlenir, etki analizi gerçekleştirilir, gerekli raporlamalar yapılır.

Platformun ilgili birimleri ile bilgi güvenliği sorumlusu aksiyon planı belirler.

a. Anlık Müdahale: Seviyesi çok ciddi olarak değerlendirilen tehdit ve risklere yönelik en kısa zamanda ve derhal aksiyonun alınır.
b. Günlük Müdahale: Seviyesi ciddi olarak değerlendirilen tehdit ve risklere yönelik bir iş günü içerisinde aksiyonun alınır.

5	**VERY SERIOUS**	The platform's system access stops completely or for an unacceptable period of time. Information integrity is irreversibly compromised. Destruction or irreversible destruction of personal data and confidential information. Significant financial loss will occur.

If recovery plans are to be implemented by the Platform, customers are informed via the website on how the recovery plans will be implemented and the related workflow procedures.

4.4. **Ensuring that all documents and records required to be kept in accordance with the legislation continue to be kept**

The Platform's secondary systems have been selected so as not to be exposed to the same risks as the primary system.

Backups of the documents and records that the Platform is obliged to keep are taken at regular intervals.

In this context, the security of all records and documents required to be kept in accordance with the legislation and MASAK legislation is ensured and loss of information, documents and data is prevented.

4.5. **Processes on how to eliminate the threat and restore system and wallet security**

In case the Platform encounters a threat of loss regarding crypto assets, information assets and systems, immediate action is taken.

Within this framework, the threat is first identified, impact analysis is performed, and necessary reports are made.

c. 3 günlük Müdahale: Seviyesi orta olarak değerlendirilen tehdit ve risklere yönelik yönelik azami 3 iş günü içerisinde aksiyon alınır.
d. Haftalık Müdahale: Seviyesi düşük olarak değerlendirilen tehdit ve risklere yönelik 5 iş günü içerisinde aksiyon alınır.

4.6. 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.

4.7. 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.

4.8. Kurulun alınan önlemler hakkında bilgilendirilmesi

Platformun operasyonel süreçlerinin etkilenmesi durumunda Kurul derhal bilgilendirilir. Bu kapsamda etki analiz raporları, alınan ve alınması planlanan önlemler ve sürece ilişkin plan Kurul'a bildirilir.

The relevant units of the Platform and the information security officer determine an action plan.

a. Immediate Intervention: Immediate action is taken as soon as possible and immediately for threats and risks whose level is considered very serious.
b. Daily Intervention: Action is taken within one business day for threats and risks whose level is considered serious.
c. 3-day Response: Action is taken within maximum 3 business days for threats and risks whose level is assessed as moderate.
d. Weekly Intervention: Action is taken within 5 business days for threats and risks whose level is assessed as low.

4.6. Tools and methods that can be used to identify the source of the weakness causing the threat or incident

Following the occurrence of the threat or elimination of the realized risk, work is carried out to identify the weakness element that caused the threat or incident. In this context, reports for the Platform's systems are examined retrospectively. All units of the Platform work together to eliminate the weakness factor.

The Platform prepares response plans for the identified risks and the prepared response plans are tested once a year and the test results are reported to the Board of Directors.

4.7. Transfer of crypto assets belonging to customers in case of a decision to discontinue operations

In this case, the Platform makes a detailed assessment. For the transfer of crypto assets belonging to customers, an agreement is made with all customers in writing or electronically in a way to replace the written form.

The transfer of crypto assets belonging to customers is carried out by prioritizing customer interests.

5. **Gözden Geçirme ve Yürürlük**

5.1. 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.

5.2. Bu Prosedürün yeterliliğinin yıllık olarak veya yönetim kurulu tarafından gerekli olduğunun takdir edilmesi halinde yıl periyodu beklenmeksizin gözden geçirilir ve gerekli değişiklikler yapılır.

5.3. Bu Prosedür, Platform'un Yönetim Kurulu tarafından onaylanarak yürürlüğe girmiştir.

4.8. **Informing the Board about the measures taken**

In the event that the operational processes of the Platform are affected, the Board shall be informed immediately. In this context, impact analysis reports, measures taken and planned to be taken and the plan regarding the process are notified to the Board.

5. **Review and Enforcement**

5.1. This Procedure is reviewed at least once a year by the Board, taking into account the processing of legislative amendments and the experience gained in practice, and necessary updates are made to the procedure.

5.2. The adequacy of this Procedure shall be reviewed annually or, if deemed necessary by the Board of Directors, without waiting for the annual period and necessary changes shall be made.

5.3. This Procedure has been approved by the Platform's Board of Directors and entered into force.