UAB CROWDPEAR
BUSINESS CONTINUITY PLAN

1. GENERAL PROVISIONS

1.1. The present business continuity plan (**"Plan"**) of UAB Crowdpear (**"Company"**) establishes :

1.1.1. The actions, duties and responsibilities of the Company's employee by ensuring and implementing the continuity of the Company's business in emergency situations;

1.1.2. The notification and troubleshooting actions in emergency situations to ensure an uninterrupted operation of the Company and limit the losses in the event of operational disruptions.

1.2. Based on the impact analysis performed by the Company, with this Plan, the Company aims to ensure that the Company's functions as a crowdfunding platform operator are carried out continuously and that risks that may have a negative impact on the Company's operations, as well as the Company's information and communication technology systems, are clearly identified in the Company.

1.3. The Manager of the Company is responsible for the implementation of the present Plan.

1.4. If the Manager the Company cannot perform his/her functions due to objective reasons (he/she is on vacation, sick, etc.), the Manager of the Company appoints an employee of the Company in advance to be responsible for the implementation of all the functions provided for in the present Plan.

2. DEFINITIONS

2.1. Unless the context requires otherwise, the capitalized definitions in the present Plan have the following meanings:

2.1.1. **Company –** UAB Crowdpear, code of legal entity 305888586, seat address: Kareivių g. 11B, Vilnius, Lithuania;

2.1.2. **Investor –** the customer of the Company who provides crowdfunding funds to the Project Owner;

2.1.3. **Law –** the Law on Crowdfunding of the Republic of Lithuania;

2.1.4. **Plan –** the present document;

2.1.5. **Platform –** the information system administered by the Company and used for crowdfunding;

2.1.6. **Project –** the project prepared and published on the Platform for business, professional, scientific, research and other needs, except for consumption, for which the Project Owner seeks to attract the crowdfunding funds;

2.1.7. **Project Owner –** the customer of the Company who seeks to attract financing for his/her Project in the Platform administered by the Company;

2.1.8. **RPO** – Recovery Point Objective, i. e., the longest period during which the data loss due to an incident is considered acceptable;

2.1.9. **RTO** – Recovery Time Objective, i. e., the longest period during which a system or process must be restored after an incident.

2.2. Other definitions used in the present Plan are understood as they are defined in the Law and other legislation of the Republic of Lithuania.

3. RISK ANALYSIS

3.1. The continuity planning of the Company’s business is based on the assessment and analysis of the possible impact on the Company’s activities. The disturbances in the Company’s activities are assessed in all cases by taking into account:

3.1.1. The financial impact;

3.1.2. The impact on the Company’s activities and/or services provided;

3.1.3. The costs that may be necessary to restore the Company’s activities and ensure continuity after the disruption of the relevant activity and/or individual function;

3.1.4. The existing preparedness of the Company to act in unforeseen circumstances;

3.1.5. The information and communication technologies necessary for the Company's activities.

3.2. The Manager of the company analyses the circumstances and situations related to the emergence of the company's operational risks and their probability periodically, but at least once a year, to ensure the continuity of the Company‘s business.

3.3. The recovery measures and preventive measures provided for in the Plan correspond to the probability of the occurrence of a possible risk and its impact on the Company's activities by evaluating them according to three levels: low, average and high.

4. PERFORMANCE IMPACT ANALYSIS

4.1. The Manager of the Company periodically performs an analysis of the impact of potential incidents on the Company's operations, during which he/she assesses the potential impact of disruptions in the Company's operations on confidentiality, integrity and availability to ensure the reliable management of continuity of the Company‘s business.

4.2. The performance impact analysis is performed on the basis of both internal and external data that may be provided by third parties (for instance, the external service providers hired by the Company).

4.3. During the performance impact analysis, the Manager of the Company also assesses the importance of the defined and classified operational functions, supporting processes, third parties and information resources and their interdependencies.

4.4. The Manager of the Company also ensures that appropriate information and communication technology systems are implemented in the company by taking into account the analysis of the impact on the activities ensuring the adequate prevention of disruptions in the Company's business and/or individual functions.

4.5. By taking into account the performance impact analysis, the Manager of the Company also decides on the need to adjust the present Plan by providing the additional measures to minimize the risk of the Company experiencing a negative impact due to disruption of the Company's activities and/or individual functions. If necessary, The Manager of the Company redefines the operational functions, supporting processes and other processes important for ensuring the continuity of business.

5. MAIN FUNCTIONS REQUIRING AN EFFECTIVE UNINTERRUPTED ASSURANCE OF BUSINESS CONTINUITY

5.1. The main functions requiring an effective uninterrupted assurance of business continuity are the following:

Function	**Possible impact on the Company's business**
The possibility for the Company's customers (Investors and Project Owners) to log in to their account on the Platform	**Average**

The representation of main information (loans, balances of funds, portfolio of granted loans) in the Platform accounts of the Company‘s customers (Investors and Project Owners)	**Low**
The possibility for the Company's customers to perform basic operations – to finance and receive financing for Projects	**High**
Uninterrupted registration and storage of information about the Company's customers and their transactions	**Average**
Management of the Company's business operations	**Average**
Identification of the Company‘s customers (Investors and Project Owners)	**High**

5.2. During the performance impact analysis, the Company has identified the business processes listed below with a significant impact on the Company's operations:

	Business process	**Description**
	Customer registration / service	
1.	Customer registration	Continuous registration of the Company‘s customer (Investor or Project Owner) and data storage
2.	Customer identification (KYC process)	Continuous customer identification (KYC) procedure including the collection of necessary information and data and the use of identification means in accordance with the Company's money laundering prevention procedures
3.	Customer log in	The possibility for the Company's customers (Investors or Project Owners) to log in to their Platform accounts
	Project publication and financing	
4.	Project development	The possibility for the Project Owners to provide information about their Projects and publish it on the Company's Platform after the Company's evaluation
5.	Update of Project information	The possibility for the Project Owners to update the information about their Projects published in the Company‘s Platform
6.	Deposit of funds	The possibility for the Investors to deposit the funds to their payment accounts (operated by an external payment service provider) to invest these funds in projects published on the Platform, as well as the possibility for the Project Owners to deposit the funds to their payment accounts (operated by an external payment service provider) to use these funds for the payment of fees imposed by the Company
7.	Withdrawal of funds	The possibility for the Investors to withdraw the funds from their payment accounts (operated by an external payment service provider) for the funding of Projects published in the Company‘s Platform, as well as the

		possibility for the Project Owners to withdraw the funds from their payment accounts (operated by an external payment service provider), which were received as a loan after the successful financing of the Project on the Platform or deposited by the Project Owner (for instance, to pay the applicable fees)
8.	Project funding	The possibility for the Investors to invest in the Projects published in the Company‘s Platform
9.	Transfer of the funds to the Project Owner	The possibility to transfer the funds collected after the successful financing of the Project to the Project Owner
10.	Payment of interest to the Investors	The possibility for the Project Owners to pay interest (as well as any other fees payable to the Investors or the Company) according to the loan agreements concluded on the Platform
	Customer account support	
11.	Account password change process	The possibility for the customers to change the passwords used to log in to the accounts registered in the Platform
12.	Contact information update	The possibility for the customers to update their contact information provided during the registration in the Platform
13.	Submission of information about the Projects	The possibility to provide the information about the projects in which the customers have invested or are their owners to the Company‘s customers (in their accounts registered in the Platform)
	Data storage	
14.	Data storage	The possibility for the Company to store the information about the Company's customers, their operations, financed projects and any other information related to the Company's activities securely
	Customer service	
15.	Handling of customer complaints	The possibility to receive the customer complaints and handle them properly
	Sale process	
16.	Making of the offers	The possibility to provide the financing terms to potential customers of the Company (Project Owners)
17.	Negotiation process	The possibility to conduct negotiations with potential customers of the Company (Project Owners) properly
	Accounting	
18.	Accounting process	The possibility to conduct the accounting procedures in the Company's activities properly

19.	Invoicing process	The possibility to issue the invoices to the Company‘s customers and associated parties properly

6. MEASURES ENSURING THE UNINTERRUPTED BUSINESS

6.1. The Company takes into account the operational risks that it may encounter during its business to ensure its uninterrupted operation as a crowdfunding platform operator.

6.2. The Company identifies the following operational risks as the main risks:

6.2.1. The inability of the Company's employees to perform their functions;

6.2.2. The loss of the Company‘s premises;

6.2.3. Hardware failures;

6.2.4. Cyber-attacks;

6.2.5. Platform functionality disorder;

6.2.6. Data loss;

6.2.7. The disruptions in activities of payment and identification service providers.

6.3. The Company understands that the list of risks specified in Clause 6.2 of the present Plan is not exhaustive. If other operational risks of the Company (not directly mentioned in this Plan) occur, the Company's employees must respond appropriately in accordance with the general principles and procedures provided for in the present Plan.

6.4. If the Company faces the solvency problems or the Company is at risk of bankruptcy, another entity that can perform the functions of the crowdfunding platform operator is searched for as quickly as possible in accordance with the procedure provided by the Law. The transfer of the administration of the Platform to another entity with the right to administer the crowdfunding platform cannot in any way worsen the situation of the Company's customers (Investors and Project Owners).

7. INABILITY OF THE COMPANY‘S EMPLOYEES TO PERFORM THEIR FUNCTIONS

7.1. The Manager of the Company must ensure that in cases where the Company's employees are unable to perform their functions for any reason, their functions could be immediately taken over by another employee of the Company or the Manager of the Company, until the necessary need for employees to perform the functions in the Company's activities is restored.

7.2. In case of inability to perform his/her functions of the Company‘s employee, the damages, if any, are assessed.

7.3. In case of inability to perform his/her functions of the Company‘s employee, the Manager of the Company immediately but no later than within 1 (one) business days assesses whether:

7.3.1. The failure to perform the functions of the Company's employees may affect the Company's performance, i. e.:

7.3.1.1. The conclusion of crowdfunding transactions in the Platform administered by the Company;

7.3.1.2. The reliability assessment process of the Project Owners;

7.3.1.3. The implementation of money laundering and terrorist financing prevention requirements and related procedures;

7.3.1.4. The administration of crowdfunding transaction concluded in the Platform;

7.3.1.5. The execution of communication with Company‘s customers (Investors, Project Owners);

7.3.1.6. Other functions implemented by the Company in carrying out its activities and providing crowdfunding services.

7.3.2. The functions of an employee of the Company could be transferred to another employee of the Company;

7.3.3. There is a need to hire another employee to perform the required work functions.

7.4. In case of an extremely urgent and immediate need for personnel, the Manager of the Company is looking for alternatives (for example, to purchase a service from third parties, to hire employees) until the necessary employee is found. The respective alternatives must be implemented within 2 (two) weeks at the latest. Until the services are started to provide or an employee is hired, the necessary functions must be proportionally distributed to other (existing) employees of the Company immediately, but no later than within 1 business day.

7.5. After having performed the assessment specified in the Clause 7.3 (and, if necessary, after having hired another employee), the Manager of the Company transfers the functions of an employee of the Company who is unable to perform his/her functions to other employee(s) and/or an external service provider.

7.6. Until the situation related to the inability of the Company's employee(s) to perform their functions is fully restored in the Company, the Manager of the Company must constantly monitor whether the measures taken to ensure the performance of the relevant functions allow the Company to carry out its activities at least to the extent that would ensure the proper provision of crowdfunding services.

7.7. The Manager of the Company must regularly (at least 1 (one) time per month) assess whether the Company has the possibility to distribute the functions of each employee to other employees of the Company preventively, if some employee of the Company could not perform his/her functions for certain reasons, and whether such distribution of functions to other employees of the Company would ensure the proper provision of crowdfunding services and related processes until the initial situation is restored.

7.8. The documents and information with which employees work must be available to the Company or at least one other employee (for instance, stored on a cloud server, stored in physical or electronic form by providing permanent access to the Company's Manager or another employee) to ensure the possibility for the Manager of the Company or another employee to take over the employee's functions.

7.9. In terms of risk, the Company assesses that the inability of the Company's employees to perform their functions is of medium probability (low probability for the period longer than 1 business day) and the potential adverse effects are low.

7.10. In case of inability of employees to perform their functions, the Company establishes RTO of 1 hour and RPO of 0,5 hour.

8. RECOVER OF THE COMPANY‘S BUSINESS IN CASE OF LOSS OF THE COMPANY’S PREMISES

8.1. In case of loss of premises (fire, natural disaster, act of terrorism, criminal acts or other actions), the people are being evacuated first of all.

8.2. The Manager of the Company or a person authorized by him/her makes a decision on further actions necessary to continue the operational processes and avoid the loss of company documents, assesses the damage suffered, restores technical means and connections, as well as immediately informs the persons responsible for server and IT maintenance and the necessary emergency services.

8.3. If the Company loses its premises, the Manager of the Company must organize the Company's remote work or work from temporary premises as soon as possible. The creation of these alternative working conditions must be implemented no later than within 1 business day. The Manager of the Company must also ensure that the selected method of work organization (remote work, work from temporary premises, etc.) allows employees to fulfil their functions in full and that the corresponding

work organization method does not limit the provision of important functions in the Company's activities.

8.4. The Manager of the Company must ensure that the documents used in the Company's activities essential for the Company's operations or service provision are regularly scanned and stored electronically on the Company's servers.

8.5. The documents used for the Company's daily activities must be kept in locked cabinets. If necessary, The Company's activity documents may be transferred to a third party with whom the Company has concluded a document archiving agreement.

8.6. The maximum recovery time in case of loss of premises is 24 hours.

8.7. The Manager of the Company must take preventive measures, i.e., ensure that at least 2/3 of the Company's employees have laptops and access to the Internet providing the possibility for the Company's employees to perform their functions remotely to ensure the recovery of the Company's activities in case of loss of premises.

8.8. In terms of risk, the Company assesses that the loss of premises is of low probability and the potential adverse effects are medium.

8.9. In case of loss of the premises, the Company establishes RTO of 1 hour and RPO of 0,5 hour.

9. HARDWARE FAILURES OR MALFUNCTIONS

Power failure

9.1. In case of a power failure, the first employee of the Company who notices it must immediately inform the Manager of the Company.

9.2. The Manager of the Company evaluates the situation and immediately informs the owner of the Company's premises and the building administrator about the power supply failure. The Manager of the Company also communicates with the owners of the premises and/or the administrator of the building regarding the expected time of restoration of electricity supply and informs the Company's employees about it.

9.3. If the electricity supply is not restored within 4 hours, the Manager of the Company can inform about the evacuation of workplaces and organize work as provided in the Clause 8.3 of the present Plan (for instance, remotely).

9.4. The Manager of the Company preventively ensures that at least 2/3 of the Company's employees have laptops enabling them to work outside the Company's premises in the event of a power failure.

9.5. In terms of risk, the Company assesses that the power failure is of low probability and the potential adverse effects are low.

Hardware malfunctions

9.6. The Manager of the Company ensures that in case of failure of the hardware required for the performance of the functions of the Company's employees, it is possible to use spare technical equipment or that the technical equipment is repaired or replaced within 24 hours.

9.7. Respectively, the Manager of the Company must ensure that at least 1/3 of the employees are provided with spare hardware (for instance, laptops, mobile phones or other equipment necessary for the functions of employee).

9.8. In terms of risk, the Company assesses that the hardware malfunctions are of medium probability and the potential adverse effects are low.

Internet connection supply failures

9.9. IT service provider used by the Company ensures the continuity of information system operations. If the Internet connection with the Company's servers is interrupted due to a communication service

failure, the Manager of the Company informs the operator providing the Internet connection to the Company immediately and makes every effort to restore the Internet connection supply.

9.10. If the provision of communication services is not recovered within 4 hours, the Manager of the Company must use an alternative communication service provider (able to offer a quick and safe technical solution). In the absence of any real alternatives for the provision of communication services, the Manager may announce the evacuation of workplaces and organize work as provided for in the Clause 8.3 of the Plan.

9.11. In case of hardware failure or malfunction, the Company establishes RTO of the next business day and RPO in the real time.

10. CYBER-ATTACKS AND IT TECHNOLOGY DISRUPTIONS

10.1. An employee of the Company who notices a cyber-attack carried out or occurred against the Company or detects a virus of any kind in the Company's systems must immediately report it to the Head of the Company's IT Department.

10.2. After having received the notice specified in the Clause 10.1 of the Plan, the Head of IT Department must take the following actions immediately, but no later than within 2 hours:

10.2.1. Assess the possible impact of a cyber-attack and/or virus, the causes of its occurrence and contact the IT service providers used by the Company;

10.2.2. Take any further steps necessary to restore the affected functions and/or services of the Company;

10.2.3. Informs the Manager of the Company about the received notice.

10.3. After having performed the assessment specified in the Clause 10.2.1 of the Plan, the Head of the Company's IT Department prepares a plan of measures that can be implemented to avoid similar type of cyber-attacks or viruses in the future and submits this plan to the Manager of the Company who is responsible for its implementation. If necessary, the Head of the Company's IT department and the Manager of the Company consult with IT service providers and specialists for the preparation and implementation of relevant plans and measures.

10.4. In consultation with the Head of the IT department or external service providers, the Manager of the Company must ensure the implementation of the following preventive measures to avoid the cyber-attacks or viruses:

10.4.1. periodic training of the Company's employees on cyber security issues. These trainings must be organized at least once a year. The Manager of the Company can use cyber security specialists for training;

10.4.2. to select the reliable and well-known IT service providers in the market who would ensure the protection of the Company's IT systems against cyber-attacks and/or viruses to the maximum;

10.4.3. to use IT service providers for periodic security audits of IT systems, during which the security of the Company's IT systems in relation to cyber-attacks and viruses would be assessed. The security audit of IT systems must be performed in the Company at least once a year.

10.5. The Company applies the following preventive measures in its activities helping to avoid cyber-attacks:

10.5.1. the employee training focused on the types of cyber-attacks, their recognition and detection capabilities, preventive actions to avoid viruses, etc.;

10.5.2. ensures the use of all essential IT solutions protecting the Company from cyber-attacks and/or viruses in the Company, including but not limited to firewalls and anti-virus programs;

10.5.3. selects the reliable IT service providers and periodically performs security analysis of IT systems.

10.6. Inter alia, the Company follows the following principles and security measures in all cases when using IT solutions in its activities:

10.6.1. **IP filtering**. The administrative (control) areas of the IT systems used by the Company can only be accessed with pre-approved IP addresses. The persons and points of contact to which access is granted are determined for this purpose (for instance, only IP addresses of predefined workplaces are allowed to connect, a virtual private network (VPN) is used;

10.6.2. **Limited access**. The Company does not have the possibility to connect to the databases used by the Company externally. Only pre-approved persons from pre-known locations can access the databases used by the Company;

10.6.3. **Encryption (SSL certificate)**. The Company's website where the Company's services will be available will work with the help of an SSL (Secure Sockets Layer) certificate. SSL certificate, inter alia, will help to encrypt the information sent between the client and the platform server. The browsing and other actions performed on the Company's website are encrypted by using an SSL certificate;

10.6.4. **Monitoring**. The system is installed on the Company's website that can be used to monitor the user logins (login/logout time and date) and see user actions (editable elements, confirmations, instructions, payments);

10.6.5. **Passwords**. The Company's clients will be required to increase the complexity of their passwords to protect against fraud and other operational risks, i. e., the passwords must be complex, consisting of 8 or more characters, including upper- and lower-case letters, numbers and additional special characters. The secondary password (two-factor authentication) technology is used additionally.

10.6.6. **Login protection**. The firewalls are used in all cases when connecting to the external network by the Company's employees and systems.

10.7. In terms of risk, the Company assesses that the cyber-attacks and IT technology disruptions are of low probability and the potential adverse effects are medium.

10.8. In case of cyber-attacks and IT technology disruptions, the Company establishes RTO of 1 hour and RPO of 0,5 hour.

11. MALFUNCTIONS OF PLATFORM FUNCTIONALITY

11.1. If the operation of the Platform managed by the Company is disrupted, the employee of the Company, who notices this, must immediately report about it to the Manager of the Company. The Manager takes appropriate measures to inform the Company's clients of the Platform or its operational malfunctions immediately, but no later than within 12 hours.

11.2. If the Platform operation is disrupted, The Manager of the Company must contact the Company's IT service provider with a request to eliminate malfunctions of the Platform or its respective functionalities immediately, but no later than within 2 hours.

11.3. If it was not possible to finance the Projects published on the Platform due to malfunctions of the Platform or its functionality, the financing term of the corresponding Projects published on the Platform may be additionally extended (corresponding to the time of the mentioned Platform or its functionality malfunctions) by the order of the Manager of the Company. All the Company's clients are immediately informed about such a decision.

11.4. It must be noted that the Company's Platform is one of the essential IT solutions used in the Company's activities and its proper functioning is essential for the provision of the Company's services. Accordingly, the Company has chosen a Platform licensing solution.

11.5. Considering the fact that the Company has chosen to license the Platform, the Company implements the following additional preventive measures to ensure the continuity of the Platform activities:

11.5.1. verifies the reliability of the service provider;

11.5.2. ensures that in case of Platform malfunctions, the Company can promptly communicate with the relevant service provider from which the Platform is licensed;

11.5.3. establishes the provisions in the Platform licensing agreement ensuring the obligations of the service provider to properly and timely eliminate any malfunctions of the Platform and responsibility for non-compliance with the relevant obligations.

11.6. In case of any malfunction of the Platform and/or its separate functionality, the Company contacts the service provider licensing the Platform immediately, demands to eliminate the relevant disruption in the shortest possible time and restore the Platform's operation so that the Company can continue to provide its services properly.

11.7. The Company also ensures that all companies related to it or owned by the Company carrying out or intending to carry out the crowdfunding activities conclude separate (independent) licensing agreements with the external service provider providing the Platform solution.

11.8. The Manager of the Company or a person authorised by him/her informs the Company's customers in advance about the planned updating, replacement or maintenance of the Platform that may disrupt the operation of the Platform by publishing the relevant information on the Platform.

11.9. In terms of risk and taking into account the fact that the Platform is licensed from a reliable service provider, the Company assesses the probability level as low, however, the risk of potential adverse effects in the event of Platform disruptions is high.

11.10. In case of Platform functionality malfunctions, the Company establishes RTO of 1 hour and RPO of 0,5 hour.

12. DATA LOSS

12.1. To protect against the consequences of data loss incidents, the Manager of the Company implements technical measures to ensure the data security in the Company's activities enabling:

12.1.1. to copy and store the information that the Company and its employees use in their activities on the external and/or internal server of the Company periodically (at least once a day);

12.1.2. to recover the lost data and information no later than within 24 hours.

12.2. In case of data loss, the entities providing server administration services to the Company and/or entities providing IT services to the Company are informed (depending on the nature of data loss) and a specific deadline for data recovery is established that cannot be longer than 24 hours.

12.3. In case of an incident where data is potentially leaked or intercepted by third parties (when any unauthorized access to data by the Company is possible), the Manager of the Company must carry out the following actions within at least 24 hours:

12.3.1. To assess the type and volume of data leaked or intercepted during the respective incident;

12.3.2. To determine whether personal data was leaked (or could have been leaked) or intercepted (or could have been intercepted) to any extent during the incident. If so, the Manager of the Company and other employees of the Company follow the procedures provided for in the General Data Protection Regulation and the personal data breach management rules approved by the Company regarding the possible personal data breach (in addition, the State Data Protection Inspectorate is immediately informed about the breach of personal data protection);

12.3.3. To take steps to find out how the security of the data was compromised and to fix the security breach;

12.3.4. To block accounts whose logins may have been exposed due to the vulnerability and take steps to change those accounts' logins;

12.3.5. To notify the Company's clients immediately about the temporary disruptions of the Platform, if the Platform's functions are temporarily limited due to the change;

12.3.6. To assess the need to submit legal claims to third parties, apply to law enforcement and pre-trial investigation institutions.

12.4. In terms of risk, the Company assesses the data loss probability as low and its possible potential adverse effects as medium.

12.5. In case of data loss, the Company establishes RTO of 1 hour and RPO of 0,5 hour.

13. DISRUPTIONS OF THE SERVICE PROVIDER ACTIVITIES

13.1. To avoid disruptions in the activities of the service providers used (for example, due to disruptions in the activities of payment and/or customer identification service providers) or termination of the cooperation of the relevant entities with the Company, the Company takes the following preventive actions:

13.1.1. To keep in constant contact with alternative service providers and know the scope of services they can provide. If possible, to enter into contracts with several service providers;

13.1.2. To monitor whether the service providers properly implement the service provision levels set in the contracts concluded with them constantly;

13.1.3. To ensure that the contracts entered into with the service providers contain the provisions related to the deadlines for the restoration of malfunctions, the submission of notices about malfunctions, etc.

13.1.4. To ensure continuous monitoring of services provided by the service providers;

13.1.5. To ensure that in case of disruptions of the aforementioned functions, the Company could transfer the provision of services (in full or at least partially) to another service provider.

13.2. In case of disruptions of the payment service provider activities, the Manager of the Company contacts the service provider and clarifies the reasons for the disruption and the deadlines for their elimination immediately, but no later than within 2 hours. If it is established that the disruption cannot be eliminated within a few hours, the Company, if possible, directs the collected payments to another payment service provider (to an account opened in its system for the administration of crowdfunding funds) and informs the Company‘s clients about it immediately, but no later than within 4 hours.

13.3. If the payment partner withholds the funds payable to the Company's clients for more than 24 hours, the additional financing of the Company may be initiated, if necessary, by ensuring the timely settlement with clients. Such financing must be executed within 24 hours at most.

13.4. If the activity of the service provider helping to identify the clients is disrupted, the Manager of the Company takes measures to stop the registration of new customers on the Platform and to prevent unidentified clients from providing financing through the Platform. The Manager of the Company contacts the service provider and clarifies the reasons for the malfunction and the deadlines for their elimination immediately, but no later than within 2 hours. If it is established that the disruption cannot be eliminated within 4 hours, the Company may identify the client itself (for example, identify the client physically) or refer the clients to another service provider's system that provides identification services.

13.5. In all cases of disruption of activity of the service providers, the Manager of the Company must immediately assess whether the Company has the technical capabilities and readiness to take over the services provided by the service providers and perform them with internal resources (for instance, to evaluate the possibilities of determining the identity of a part of the clients physically with their presence or remotely as permitted by legislation, etc.), if the Company is entitled to provide such services (for instance, it should be taken into account that the Company is not entitled to provide payment services).

13.6. If the Company does not have the technical capabilities to take over the services provided by the service providers or is not entitled to provide the respective services, the Manager of the Company applies to an alternative service provider and aims to conclude a contract for the provision of respective services as soon as possible, but no later than within 48 hours.

13.7. In terms of risk, the Company assesses the probability of disruptions of service provider activities as low, but the level of adverse effects of such disruptions may be high.

13.8. In case of disruptions of service provider activities, the Company establishes RTO of the next business day and RPO in the real time.

14. DEVELOPMENT OF RESPONSE AND RECOVERY PLANS

14.1. Following the analysis of the impact on its operations, the Company prepares response and recovery plans foreseeing the conditions under which they are applied and what actions need to be taken to ensure the availability, continuity and recovery of critical information and communication technology systems and services installed in the Company.

14.2. In its response and recovery plans, the Company provides the short-term and long-term recovery scenarios by evaluating alternatives where the short-term recovery may not be possible due to cost, risk, logistics, or other unforeseen circumstances.

14.3. The following requirements apply to the response and recovery plans prepared by the Company:

14.3.1. The plans are prepared by taking into account the recovery of the Company's critical operational functions, supporting processes, information resources and their interdependence relationships to avoid the negative effects on the Company's operations and financial system;

14.3.2. The plans are registered and the Company's employees are given the opportunity to easily access them in an unforeseen event;

14.3.3. The plans are updated based on experience gained from incidents and testing, identified risks and threats, as well as changes in recovery objectives and priorities;

14.3.4. The plans include expected continuity measures that mitigate the disruptions to the activities of third parties and are extremely important for the continuity of the Company's information and communication technology services.

14.4. The Manager of the Company is responsible for the proper implementation of the provisions of this section.

15. SOLVENCY ISSUES, BANKRUPTCY RISK OR OTHER CAUSES DUE TO WHICH THE COMPANY CANNOT CONTINUE ITS BUSINESS

15.1. If the Company faces uncontrollable solvency issues, a real risk of bankruptcy or other circumstances due to which the Company cannot properly carry out its activities, the Company:

15.1.1. informs the Bank of Lithuania (supervising authority) about this situation immediately by detailing the current level of risk, the risk management measures used or planned to use and measures to ensure the business continuity;

15.1.2. cancels the Projects published on the Platform for which funding is being collected immediately, as well as no longer enter into or enable new crowdfunding transactions (the funds of such Investors are returned back to these Investors);

15.1.3. searches for another entity that can perform the functions of the crowdfunding platform operator in accordance with the procedure established by the Law immediately. The transfer of the administration of the Platform to another entity with the right to administer the crowdfunding platform cannot in any way worsen the situation of the Company's clients (Investors and Project Owners).

15.2. The Project Owners and Investors conclude crowdfunding transactions (loan agreements) on the Platform among themselves. Therefore, even in cases where the Company is no longer able to carry out the activities of the crowdfunding platform operator, the Project Owners must continue to properly fulfil their obligations to the Investors arising from the crowdfunding transactions (loan agreements). In such case, the Company:

15.2.1. Provides the Investors with available information about crowdfunding transactions (loan agreements) concluded by them and their execution progress. Thus, the conditions are created for the Investors to directly carry out the administration and collection processes of the loans they have granted to the Project Owners;

15.2.2. informs the Project Owners that the administration of the concluded and executed crowdfunding transactions (loan agreements) will continue to be carried out on behalf of the Investors, not by the Company, but by the Investors themselves (or their appointed another entity). The Project Owners are provided with the information they need to fulfil their obligations directly to the Investors.

16. CONTACT PERSONS

16.1. The Company approves and provides employees with a list of contact persons who must be contacted immediately in the event of a specific disruption of the Company's business. If the Company's employees identify any malfunction of the Company's business, the Manager of the Company is immediately informed in all cases, in addition to the contact persons specified in the relevant list.

16.2. In case of a specific malfunction of the Company‘s business, the Manager of the Company must immediately inform the Company's clients (Investors and Project Owners) and/or other interested parties about it.

16.3. If the contact details change, the Manager of the Company updates the information provided in the list of contact persons immediately and introduces it in writing to all employees of the Company.

17. FINAL PROVISIONS

17.1. The employees of the Company must be familiarized with their functions and duties provided for in the present Plan by signature. The Manager of the Company is responsible for the familiarization of the employees with the Plan.

17.2. The Manager of the Company is responsible for periodic (at least once a year) testing and updating of the Plan. The results of the tests must be documented and all deficiencies identified during the tests must be analysed and eliminated.

17.3. The Plan is approved, updated or amended by order of the Manager of the Company.

17.4. The Plan and/or its updates and changes must enter into force on the day of the adoption of the order of the Manager of the Company, unless the law provides for a different date of entry into force.