Form 2.1

BUSINESS CONTINUITY PLAN

1. GENERAL PROVISIONS

1.1. The Business Continuity Plan of Sutelktinio finansavimo platforma Profitus UAB (hereinafter referred to as the "**Company**") (hereinafter referred to as the "Plan") shall be aimed at establishing the measures and procedures intended for continuous operation of the Company and provision of services in unforeseen situations.

1.2. The terms used herein shall be construed as defined in the Rules and the Republic of Lithuania Law on Crowdfunding unless otherwise specified herein.

1.3. This Plan shall be followed by the Company.

1.4. The Plan shall be drawn up in accordance with the Republic of Lithuania Law on Crowdfunding and the accompanying implementing legal acts.

2. DEFINITIONS

2.1. Unless the context requires otherwise, for the purposes of this Plan, the capitalised works and expressions shall have the following meanings:

2.1.1. "**Platform of the Company**" shall mean an information system administered by crowdfunding operator through which crowdfunding is carried out.

2.1.2. "**Investor**" shall mean a person who provides crowdfunding funds to the Project Owner.

2.1.3. "**Law**" shall mean the Republic of Lithuania Law on Crowdfunding.

2.1.4. "**Project**" shall mean a project prepared for meeting business, professional, scientific, research or other needs, except for consumption, to be published and/or published on the Platform, for the purposes of implementation of which the Project Owner seeks to raise crowdfunding funds.

2.1.5. "**Project Owner**" shall mean the person who initiates and announces a project for investors thought the Platform.

2.1.6. "**Manager**" shall mean the director of the Company.

3. ORGANISATIONAL PROVISIONS

3.1. In the event of occurrence of an event or incident (emergency) which has significantly damaged or may damage the Company's business processes, the employee detecting the event shall immediately notify the Manager or another person authorised thereby.

3.2. In the event of occurrence of an event or incident, the Manager of the Company shall be entitled to set up the Business Continuity Management Group which shall carry out the business continuity management actions or an authorised person shall act according to the Plan (hereinafter all aforementioned persons shall be referred to as the "Acting Persons"). The Acting Persons shall:

3.2.1. analyse events and incidents, take decisions on the issues concerning business continuity management;

3.2.2. communicate with the representatives of the producers/disseminators of public information;

3.2.3. communicate with law enforcement and other institutions;

3.2.4. ensure security of information in the event of occurrence of an incident;

3.2.5. submit reports on the business continuity management to the Manager of the Company;

3.2.6. fulfil other assigned functions.

3.3. The Acting Persons shall communicate with each other by telephone, e-mail and/or via the internal communication program of the Company.

3.4. When dealing with an emergency the Company shall rely on the knowledge and competence of the employees by information processing and communication means (data, server and computer equipment and hardware, computer and telephone network installation and active equipment), the employees of the company which carries out management and supervision of technical measures of the Company and available technical measures and, if necessary, the services of third parties.

3.5. Typical actions of response to an emergency shall be as follows:

3.5.1. assessment of the sustained damage, taking of a decision on initiation of the business continuity plan, warning of the Company's employees, the Investors and the Project Owners;

3.5.2. carrying out of urgent actions ensuring continuation of the operational processes in an emergency mode;

3.5.3. restoration of critical operational processes lasting not longer than for 24 hours;

3.5.4. rectification of the emergency;

3.5.5. establishment/elimination of the reasons;

3.5.6. recording of the incident in the register of operational events;

3.5.7. introduction of preventive measures.

3.6. In the event of occurrence of an incident, the maximum amount of data which may be lost shall be the data of the last 24 hours. The afore-mentioned data shall include all operations carried out by the customers throughout the entire period.

3.7. The Company shall consider the following as the critical processes:

3.7.1. the possibility for the customers to log in to their Investor and/or Project Owner account on the Platform of the Company;

3.7.2. representation of the main information (loans, balances of funds, portfolio of granted loans) in the Investor and/or Project Owner account;

3.7.3. performance of main operations (to be financed and financing) for the Investor and/or the Project Owner.

3.8. The methods, means and actions used for implementation of the Plan shall be adequate to the particular situation.

3.9. The methods, means and actions used for implementation of the Plan shall be effective in terms of costs and increase direct or indirect economic benefit.

3.10. All incidents related to the Company's business continuity shall be recorded in the register of operational events of the Company.

4. UNDERLYING OPERATIONAL RISKS OF THE COMPANY:

4.1. The underlying operational risks which may affect the Company's activities shall be as follows:

4.1.1. Loss of the premises of the Company;

4.1.2. Loss of the Company's employees;

4.1.3. Malfunctions and failures of transmission of data;

4.1.4. Failures of communication services;

4.1.5. Malfunctions of technical equipment;

4.1.6. Malfunctions of the Platform;

4.1.7. Loss/disclosure of data (social engineering events);

4.1.8. Failures of payments, identification partners;

4.1.9. Removal of the Company from the public list of crowdfunding operators;

4.1.10. Insolvency (bankruptcy or restructuring) of the Company or termination of activities.

5. RESTORATION OF THE ACTIVITIES OF THE COMPANY IN THE EVENT OF LOSS OF THE PREMISES OR LOSS OF EMPLOYEES

5.1. In case of loss of the Company's premises (fire, natural disaster, terrorist act, criminal acts or other actions), first of all, evacuation of people shall be carried out; the Manager or an authorised person thereof shall take a decision on further actions necessary for continuation of operational processes, adopt measures with a view to avoiding physical loss of the Company's documents, assess the sustained damage; technical means and communications shall be restored in accordance with the rules for operation and maintenance of technical means laid down in Section 6; the persons responsible for maintenance of the servers and IT and necessary emergency services shall be immediately notified.

5.2. In the event of loss of the Company's premises, the Manager of the Company shall organise the work of the Company remotely or from temporary premises.

5.3. The Manager or the authorised person thereof responsible for implementation of the Plan shall be obliged to ensure that, in order to avoid physical loss or destruction of the Company's documents as a result of a natural disaster, terrorist act, criminal acts or other actions, the documents which shall be essential to the Company's activities and/or provision of services and used in the Company's activities were scanned and electronically stored in the Company's servers, the documents used for the Company's daily activities shall be stored in locked cabinets. If necessary, the Company's operational documents may be transferred to the archive.

5.4. The maximum restoration period in case of loss of the premises before a critical situation occurs shall be 24 hours. The response shall be as follows:

5.4.1. evacuation from the building;

5.4.2. reporting to the respective services (fire service, police etc.);

5.4.3. remote organisation of the employees' work;

5.4.4. if necessary, the premises for ensuring proper working environment are recommended and temporary or simply new premises for the office shall be sought.

5.5. In the event of loss of employees of the Company, first of all, the sustained damage (if any) shall be assessed. The Manager shall assess if:

5.5.1. loss of personnel may have an impact on performance of the Company's activities;

5.5.2. what functions of the lost personnel could be transferred to another employee of the Company;

5.5.3. if the need for employment of another employee (other employees) for fulfilment of the functions of the lost personnel exists;

5.5.4. in the event of urgent need for personnel, the Manager shall seek for alternatives (for example, purchase of the service from third persons, hiring out of employees) till necessary personnel are found. Necessary functions shall be distributed among other employees of the Company before starting providing the services or the employee is employed.

6. MANAGEMENT AND SUPERVISION OF TECHNICAL MALFUNCTIONS, DATA LOSS, COMMUNICATION MEANS, PLATFORM MALFUNCTIONS IN THE EVENT OF AN EMERGENCY

6.1. Management and supervision of technical malfunctions, data transmission, communication malfunctions, platform malfunctions shall be aimed at ensuring that, in the event of a failure of the Platform of the Company, systems, databases (malfunctions of the Internet, malfunctions of the IT systems or software, cyberattacks), all managed data and information or the major part of data and information were restored as soon as possible and after the malfunctions, the Company's platform and system would further operated.

6.2. The liability for proper organisation of supervision and management of the afore-mentioned measures shall fall within the Manager of the Company or an authorised person thereof or a third party providing such services.

6.3. The Company shall use the following measures for protection against damage to the software and loss of data:

6.3.1. Making copies of information available in the Company's server (including system folders). Backup copies of the virtual server shall be made, i.e. all information available in the Company's server shall be copied, on a daily basis from 2:00 to 3:00. Thus, restoration of all data or the major part of the data available in the Company's service in case of unforeseen circumstances shall be ensured;

6.3.2. The Company shall also use a virtual server meeting the standards ISO 27001 and ISO 27018;

6.3.3. The Company shall store data in remote data centres meeting the standard ISO 27001.

6.3.4. Copies of the Company's databases shall be made on a daily basis from 23:00 to 24:00 (copies of the day) and on the 30th day of each month from 2:00 to 3:00 (copies of the month). When the moment of damage to the data is established, the damaged data from bulk data shall be replaced with the most recent available good data. Thus, restoration of all entries or the major part of entries in the Company's databases in the event of unforeseen circumstances shall be ensured;

6.3.5. In order to protect the system against cyberattacks, data reading, all information shall be accessible using virtual private network (VPN) logins. The Platform maintenance specialists shall encode passwords before sending them to the database; important actions on the page shall be additionally stored subject to the password request. The customers shall be requested to ensure increased complexity of passwords (at least 8 symbols including a figure, special symbol and/or at least one lower-case and upper-case letters), regularly change them.

6.4. The Company's employees shall use portable and desktop computers (Apple or meeting similar standards) which shall be connected to the Company's servers. Therefore, in case of any malfunctions of the Internet in the Company's premises, the Company's activities may be moved to other premises (for example, home) and, in case of loss of equipment, important information shall be saved. Malfunctions of the Internet shall not have an impact on operation of the Company's datacentres, servers (the server used by the Company shall be in the datacentre).

6.5. The Company shall seek that, in case of malfunctions, all reasonable measures to minimise the amount of lost data and restore operation of the Platform of the Company within the time limits specified in the Plan shall be assumed. Attempts shall be made that the maximum amount of lost data was not higher than the amount of data obtained during 24 hours.

6.6. At the decision of the Manager, management, supervision of technical measures, maintenance of information processing systems and ensuring of the continuity of operation thereof may be transmitted to another legal person who must ensure proper fulfilment of the functions assigned to it and continuity of the Company's services, operation of the systems and infrastructure. In case of delegation of the function, the contact details of such legal person shall be attached as an annex hereto. The operations manager of the Company shall be liable for the failure to ensure or improper ensuring of the continuity of operation of the systems and infrastructure by the selected legal person.

6.7. In the event of any malfunctions of the Platform (systems of the Company), first of all, the programming service providers or internal programmers of the Company shall be addressed and faults shall be sought. Later on, if no programming errors are detected, the server (database) service providers shall be addressed.

6.8. In case of any communication malfunction in the premises, mobile internet communication may be organised by a decision of the manager of the Company.

6.9. The maximum restoration time before a critical situation occurs shall be 24 hours. The response shall be as follows:

6.9.1. energy, communication or other service providers may be addressed depending on the nature of the malfunctions;

6.9.2. the programming service providers shall be notified of malfunctions (the malfunction elimination time: 2 hours);

6.9.3. server (database) service providers shall be notified (the malfunction elimination time: 2 hours);

6.9.4. if after 2 hours the malfunctions of the Platform still exist or other critical processes occur, the customers shall be notified;

6.9.5. remote work of employees may be organised.

7. LEAKAGE OF DATA (SOCIAL ENGINEERING ATTACKS)

7.1. The Company's data may be subject to risk not only due to breaches of the technical systems, communications of the Company but also due to social engineering actions where data may be lost, disclosed or access to them may be restricted.

7.2. In order to limit possible risk of social engineering attacks, the Company has approved the Information Security Procedure Description describing the requirements for work with the Company's equipment, systems, data. The Company shall also conduct training on security of information for the Company's employees.

7.3. An employee of the Company who detects a possible case of social engineering attack shall immediately notify the Manager of the Company and take reasonable actions to suspend such actions (for example, prohibit unauthorised persons from accessing the premises etc.).

7.4. In case of occurrence of such event, an investigation shall be carried out with a view to determining the reason, scope and possible consequences of the breach.

7.5. Pre-trial investigation institutions shall be immediately notified of the event, responsible employees shall be removed from office.

7.6. The response shall be as follows:

7.6.1. the manner of breach of the security shall be found out;

7.6.2. the information which has leaked shall be established;

7.6.3. the gap of security shall be filled in;

7.6.4. accounts the login data of which could be disclosed due to a gap shall be blocked;

7.6.5. data of login to the partners' accounts shall be changed;

7.6.6. the customers shall be notified of temporary malfunctions of the system if the functions of the system are temporary limited due to such change;

7.6.7. the customers shall be notified that private data of the customers could be disclosed as a result of the gap;

7.6.8. a lawsuit against a third party shall be prepared, pre-trial investigation institutions shall be addressed.

8. MALFUNCTIONS OF PAYMENT, IDENTIFICATION PARTNERS

8.1. The partners providing payment services, customer identification services shall be entitled to terminate their activities, discontinue cooperation with the Company or malfunctions in provision of their services may occur.

8.2. In pursuance of avoiding malfunctions due to the Partners' activities, the Company shall take the following actions:

8.2.1. conclude contracts with several service partners so that, in case of any malfunctions, services could be provided by another partner;

8.2.2. some services provided by the partners may be taken over by the Company itself.

8.3. In the event of any malfunctions in the payment service partner, the Manager of the Company or the authorised person thereof shall first address the Partner and try to find out the reasons of the malfunctions and the time limits for elimination thereof. In case of determining that the malfunction cannot be eliminated within several hours, if possible, the Company shall direct the collected payments to the account opened at another payment service partner institution intended for administration of the crowdfunding funds or notify the investors and request them to provide a copy of the payment order for the invested amount so that it could track the amounts of the collected crowdfunding funds.

8.4. If the payment partner retains the funds payable to the Investors or the Project Owners for more than 24 hours, if necessary, additional financing shall be ensured by the Company ensuring timely settlement.

8.5. In the event of any malfunctions in the activities of the partner helping in customer identification, the Manager of the Company or the authorised person thereof shall first address the Partner and try to find out the reasons of the malfunction and the time limits for elimination thereof. In case of determining that the malfunction cannot be eliminated within several hours, the Company shall be entitled to identify the customer (identification of the natural person) or direct customers to the system of another partner providing identification services.

8.6. The response shall be as follows:

8.6.1. the possible malfunction elimination time shall be set;

8.6.2. the customers shall be notified of the malfunctions;

8.6.3. customer identification, performance of payments shall be directed to other service providers and, if possible, carried out directly.

9. REMOVAL OF THE COMPANY FROM THE PUBLIC LIST OF CROWDFUNDING PLATFORM OPERATORS

9.1. The Company may be removed from the public list of crowdfunding platform operators in accordance with the procedure prescribed in the legislation.

9.2. In case of removal of the Company from the public list of crowdfunding platform operators, the Company's customers (Investors and Project Owners) shall be notified of the decision.

9.3. After removal of the Company from the list, the Company shall not allow to enter into new Financing Transactions. The Financing Transactions which have already been concluded shall be further performed, i.e. payments and Interest shall be accepted from the Project Owners and

distributed among the Investors, except for the cases where such obligations are transferred to other persons under the procedure prescribed in the legislation.

9.4. In cases where a request for removal from the list of crowdfunding platform operators is submitted by the Company itself, it must have concluded an agreement on the transfer of administration of financing transactions with another crowdfunding platform.

9.5. The Company shall seek to ensure that administration of the Platform of the Company was fluently transferred to another entity, i.e. so that other malfunctions of the Platform of the Company would not occur.

9.6. In case of removal of the Company from the public list of crowdfunding platform operators, the liability for proper performance of the obligations of the Company shall fall within the Manager of the Company or an authorised person thereof.

10. PROCEDURE CARRIED OUT IN THE EVENT OF INSOLVENCY OF THE COMPANY (INCLUDING THE CASES OF RESTRUCTURING)

10.1. The funds of the Investors and the Project Owners shall be kept separately from the Company's property. Therefore, in case of insolvency of the Company, the Company's creditors should not have the possibility to satisfy their claims from the property of the Company's customers.

10.2. In case of insolvency of the Company:

10.2.1. Registration of new Investors, grant of new loans and acceptance of applications from the Project Owners, conclusion of Financing Transactions shall be immediately suspended;

10.2.2. The Manager shall cooperate with the supervisory authority and the appointed administrator of the Company with a view to ensuring effective administration of the Platform of the Company or transfer thereof, cancellation of financing of the Project on the Platform.

10.3. The liability for proper fulfilment of the Company's duties in case of bankruptcy or restructuring shall fall within the Manager and/or the administrator.

10.4. In case of bankruptcy of the Company, the Financing Transactions which have already been concluded shall be deemed to be valid and must be further performed by the Parties. Administration of Financing Transactions (including mortgage transactions) shall be further administered or transferred to third parties under the procedure prescribed in the legislation.

11. FINAL PROVISIONS

11.1. This Plan shall come into force from the date of approval thereof and may be annulled or amended only by an order of the Manager.

11.2. The liability for proper compliance with the plan shall fall within the Manager or another person appointed thereby.

11.3. This Plan shall be reviewed where such need arises but at least once every two years.

11.4. The paper copy of the Plan shall be stored in the Company's premises and the electronic copy shall be stored in the Company's server.

11.5. The Company's employees shall be familiarised with the Plan and their duties provided for therein.

11.6. The authorised person of the Manager shall carry out the Plan verification procedure, i.e. testing in the course of which it shall be established if the Plan is properly complied with in the event of an unforeseen situation at least once per 12 months. During the testing, the responsible employees appointed by the Company shall analyse a possible (modelled) security incident, envisage possible ways and solutions of management thereof.

11.7. After testing the effectiveness of the Plan, the responsible employees shall prepare a report on testing the effectiveness of the management plan.

11.8. Any shortcomings noticed in the course of the testing shall be eliminated in accordance with the principle of operational efficiency, effectiveness and cost effectiveness.