Ap
proved by the order of
the head of
UAB HEAVY FINANCE
of 16 March 2022
No. HF202203-01

UAB HEAVY FINANCE BUSINESS CONTINUITY PLAN

1. GENERAL PROVISIONS

1.1. This Business Continuity Plan (hereinafter referred to as the **Plan**) of UAB HEAVY FINANCE (hereinafter referred to as the **Company**) hereby sets out the applicable measures and procedures to ensure that:

1.1.1. in the event of the Company's default, Critical Services would continue to be provided in connection with the investments made in the crowdfunding projects;

1.1.2. the agreements between the Company and the Company's customers would be properly administered;

1.1.3. in case of emergencies, the Company's activities would be uninterrupted;

1.1.4. any losses in the event of the Company's disruption are limited.

1.2. This Plan is hereby prepared according to the nature, scope and complexity of the services provided by the Company. The Head of the Company shall be responsible for the implementation of the Plan in the Company's activities. In the event that the Company is unable to perform its functions due to certain objective reasons (e.g. the manager is absent), the Head of the Company must appoint an employee of the Company in advance to perform all the functions assigned by the Company in this Plan.

2. TERMS USED IN THE PLAN

2.1. The terms used in this Plan shall have the following meanings:

2.1.1. **Company** shall mean UAB HEAVY FINANCE, legal entity code 305576227, registered office address Birutės st. 18-1, Vilnius, Lithuania;

2.1.2. **Investor** shall mean a natural person or legal entity that has submitted an investment offer through the Platform and has duly registered with the Platform;

2.1.3. **Critical Services** shall mean the Company's operational and business services, the disruption or malfunction of which would materially interfere with the Company's continued compliance with the requirements and obligations under the Regulation, impair the Company's financial results or the Company's crowdfunding services, the reliability or continuity of the Company's operations, especially with respect to Customers;

2.1.4. **Customer** shall mean the Project Owner or Investor;

2.1.5. **Plan** shall mean this Business Continuity Plan;

2.1.6. **Platform** shall mean the crowdfunding platform operated by the Company www.heavyfinance.com;

2.1.7. **Supervisory Authority** shall mean the Bank of Lithuania;

2.1.8. **Project** shall mean the Project prepared and published on the Platform for business, professional, scientific, research and other purposes, except for consumption, for the implementation of which the Project Owner seeks to attract funds from the Investors;

2.1.9. **Project Owner** shall mean a person initiating a Project intended for the satisfaction of business, professional, scientific, research and other purposes, except for consumption, and published on the Platform, for the implementation of which the Funds of Investors are required;

2.1.10. **Regulation** shall mean Regulation (EU) 2020/1503.

2.2. Other terms used in this Plan shall be understood as defined in the Regulation. Unless the context requires otherwise, the words used in the Policy shall include the singular form and vice versa.

3. RISK ANALYSIS

3.1. The Company plans the continuity of its business by assessing and analysing the potential impact on the Company's operations. Any disruption of the Company's operations shall be assessed in all cases taking into account the following:

3.1.1. financial impact on the Company;

3.1.2. impact on the Company's operations and/or services provided;

3.1.3. financial need required for the restoration of the Company's activities and/or services provided and for ensuring their continuity after the disruption of the respective activities and/or separate function;

3.1.4. Company's current readiness to act in unforeseen circumstances;

3.1.5. information and communication technologies necessary for the operation of the Company.

3.2. The Company shall take into account the risks it may face in the course of its operations in order to ensure the continuity of its operations. Such risks include, but are not limited to, the following scenarios:

3.2.1. loss of Company premises;

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

3.2.3. hardware failures;

3.2.4. Platform disruptions;

3.2.5. Data loss;

3.2.6. malfunctions of payment and identification service providers;

3.2.7. cyber attacks

3.3. In order to ensure the continuity of the Company's operations, the Head of the Company periodically, but not less than once a year, taking into account the nature, scope and complexity of services provided by the Company, shall analyse the circumstances and situations related to the Company's operational risk and probability.

3.4. The recovery and prevention measures provided for in the Plan correspond to the probability of occurrence of a potential risk and its impact on the Company's operations, assessed according to three levels: low, medium and high.

3.5. The Company has identified the following key functions that require uninterrupted business continuity

No.	Function	Potential impact on the Company's operations
1.	Key information (such as loans available, financing provided, payment terms, etc.) Customer accounts on the Platform	Low
2.	Customer login and use of the account on the Platform	Medium
3.	Uninterrupted registration and storage of information about the Company's Customers and their operations	Medium
4.	Management of the Company's business operations	Medium
5.	Execution of main operations on the Platform (funding and receipt of funding for Projects)	High
6.	Identification of the Company's Customers	High

3.6. Based on the risk analysis, the Company shall make efforts to ensure procedures to ensure the continuity of communication between the Company and the Customers, the Company's business partners, employees and the Supervisory Authority.

4. RESTORATION OF THE COMPANY'S ACTIVITIES IN CASE OF LOSS OF THE COMPANY'S PREMISES

4.1. In the event of loss of the Company's premises (e.g. in the event of a fire, military conflict, natural disaster, terrorist act, criminal offences, etc.), the evacuation of the Company's employees and other persons on the Company's premises shall be ensured first and foremost.

4.2. The Head of the Company or his/her authorised person:

4.2.1. shall decide on the further steps required to continue the business processes;

4.2.2. shall take measures to prevent the physical loss of the Company's documents;

4.2.3. shall assess the damage suffered;

4.2.4. shall take steps to re-establish technical measures and contacts;

4.2.5. shall immediately inform the persons responsible for server and IT maintenance and the necessary emergency services.

4.3. If the Company loses its premises, the Head of the Company must organise the Company's work remotely or work from temporary premises.

4.4. The Company shall, within a reasonable term, inform the Customers about the loss of the Company's premises and the significance of this loss for the Company's Customers.

5. INABILITY OF COMPANY EMPLOYEES TO PERFORM THEIR FUNCTIONS

5.1. The Head of the Company must take measures so that in cases when the employees of the Company are unable to perform their work functions for any reason, their functions may be taken over by the Head of the Company himself/herself or another employee of the Company.

5.2. In case of inability of the Company's employee to perform his/her functions, the damage suffered, if any, shall be assessed. The Head of the Company shall immediately assess whether:

5.2.1. Failure to perform the functions of the Company's employees may affect the performance of the Company's activities and /or the provision of Critical Services;

5.2.2. what functions of the Company's employee could be transferred to another employee of the Company;

5.2.3. whether there is a need to hire another employee to perform the required job functions.

5.3. After performing the assessments specified in Clauses 5.2.1 – 5.2.3, the Head of the Company may:

5.3.1. delegate an employee's job functions to another employee (s);

5.3.2. hire another employee and transfer the employee's job functions to him/her;

5.3.3. outsource the employee's work functions to an external service provider.

5.4. In the event of an extremely urgent and immediate need for an employee, the Head of the Company shall seek alternatives (e.g. purchasing services from third parties, staff leasing services) until the required employee is found. Until the start of the provision of services or the employment of an employee, the functions required to be performed must be distributed proportionally to other (existing) employees of the Company.

5.5. In order to ensure that the Head of the Company or other employee may take over the employee's functions, the documents and information with which the employees work must be permanently available to the Head of the Company or at least one other employee (e.g. stored on the Company's servers, cloud platforms, stored in physical or electronic form with permanent access to the Head of the Company or other employee).

5.6. The Company's customers shall be informed about the inability of the Company's employees to perform their functions only in exceptional cases, when after assessing the damage (if any) and determining that the employees' inability to perform their functions is essential for the Company's operations or the provision of Platform services.

6. HARDWARE FAILURES

6.1. In the event of a disruption of the electricity supply at the Company's premises, the Head of the Company or a person appointed by him/her shall immediately inform the manager of the Company's premises building. If the electricity supply is not restored within 24 hours, the Head of the Company may announce the evacuation of workplaces in order to ensure the continuity of operations.

6.2. The Head of the Company shall ensure that in case of failure of the technical equipment necessary for the performance of the functions of the Company's employees, it shall be possible to use spare technical equipment or to have the technical equipment repaired or replaced within 24 hours.

6.3. The continuity of information systems operations shall be ensured by the IT service provider engaged by the Company. If the Internet connection with the servers used by the Company is interrupted due to a failure of the communication services, the Head of the Company shall immediately inform the operator providing the Internet connection directly to the Company and

shall make every effort to restore the supply of the Internet connection. If the provision of communication services is not resumed within 24 hours, the Head of the Company must use an alternative communication service provider (who may offer an immediate and safe technical solution to resolve this situation) in order to ensure business continuity, and in the absence of any real alternative to the provision of communication services, may announce the evacuation of workplaces.

6.4. If the failures or malfunctions of the technical equipment are essential for the performance of the Company's activities or the provision of the Company's Critical Services, the Company shall inform its customers about the failures or malfunctions within a reasonable term, indicating the significance of the failures for the Company's services.

6.5. The Company's Customers shall be informed about the inability of the Company's employees to perform their functions only in exceptional cases, after assessing the damage (if any) and establishing that the employees' inability to perform their functions is essential for the Company's operations or the provision of Platform services.

7. PLATFORM DISRUPTIONS

7.1. In the event of a malfunction of the Platform or certain of its functionalities, the Company's employee shall immediately inform the Company's manager. The Head of the Company shall take appropriate measures to inform the Customers of the Company about the failures of the Platform or its activities immediately, but not later than within 12 hours.

7.2. In the event of a malfunction of the Platform, the Head of the Company shall immediately contact the Company's IT service provider with a request to eliminate the malfunction of the Platform or its respective functionalities.

7.3. In cases when due to disruptions of the Platform or its functionalities it was not possible to finance (or complete the initiated financing) projects published on the Platform, by the order of the Head of the Company, the terms of financing such projects published on the Platform may be extended additionally (according to the time of the mentioned failures of the Platform or its functionalities). All the Company's Customers shall be immediately informed about the adoption of such a decision.

7.4. The Head of the Company or a person appointed by him/her shall inform the Customers in advance about the planned renewal, replacement or maintenance works of the Platform, due to which the operation of the Platform may be disrupted, by publishing the information on the Platform.

8. DATA LOSS

8.1. In order to protect against the consequences of data loss incidents, the Head of the Company shall implement technical data security measures in the Company's operations, which create an opportunity to:

8.1.1. copy and store the information used by the Company and its employees in their activities periodically, at least once a day, on the external and/or internal server of the Company (making copies of data);

8.1.2. recover lost data and information within 24 hours.

8.2. In case of data loss, the entities providing server administration services to the Company and/or entities providing IT services to the Company shall be informed (depending on the nature of the data loss) and a specific data recovery deadline shall be set.

8.3. In the event of an incident where the data may be leaked or taken over by third parties (when any unauthorised access to the data is possible), the Head of the Company shall perform the following actions:

8.3.1. assess the volume of data leaked or intercepted during such incident;

8.3.2. determine whether personal data has been (or may have been) leaked or intercepted (or may have been intercepted) during the incident. If so, due to a possible personal data breach, the Head of the Company and other employees of the Company shall follow the General Data Protection Regulation and the personal data breach management procedures approved within the Company;

8.3.3. take action to identify breaches of data security and rectify the security gap;

8.3.4. block accounts whose login information may have been disclosed due to the gap, take action to change the login information of such accounts;

8.3.5. Customers shall be notified of temporary system failures if the change temporarily restricts system functions;

8.3.6. assess the need to bring legal actions against third parties, law enforcement and pre-trial investigation authorities.

9. DISRUPTION OF THE PAYMENT SERVICE PROVIDER AND IDENTIFICATION SERVICE PROVIDER

9.1. There is a risk in the Company's operations that external entities providing payment services and the Customer's identification services may terminate their activities or cooperation with the Company, as well as the provision of their services may be disrupted. The Company shall take the following actions to prevent disruptions due to such events:

9.1.1. has the technical capacity and readiness to take over and perform part of the services provided by the service providers with internal resources (e.g. identify some of the customers with their physical participation, etc.);

9.1.2. shall be in constant contact with alternative service providers and shall be aware of the scope of the services they can provide. Meanwhile, if possible, it shall enter into contracts with several service providers (one of which shall be the main one and the others shall be considered to be alternative). It must be ensured that in case of disruption of the aforementioned functions, the Company may transfer the provision of services (in full or at least in part) to another service provider.

9.2. In the event of a disruption of the payment service provider, the Head of the Company shall immediately contact the service provider and explain the reasons for the disruption and the terms for their rectification. If it is determined that the disruption cannot be remedied within a few hours, the Company shall, if possible, direct the collected payments to another payment service provider (to an account opened in its system for the administration of crowdfunding funds) and immediately inform the Customers thereof.

9.3. If the payment service partner withholds the funds due to the Customers for more than 24 hours, additional financing of the Company may be initiated, if necessary, ensuring timely settlement with the Customers.

9.4. In the event of a disruption in the activities of the service provider assisting in the identification of the Customer, the Head of the Company shall first contact the service provider and explain the reasons for the disruption and the terms of their rectification. If it is determined that the malfunction cannot be rectified within a few hours, the Company may identify the Customer itself (for example, by physically identifying the Customer) or refer the Customer to the system of another service provider providing identification services.

9.5. If it is not possible to direct the collected payments to another payment service provider, or if the Company and/or the service provider is unable to establish the Customer's identity, the Head of the Company shall take appropriate measures to inform the Company's Customers within a reasonable term.

10. CYBER ATTACKS AND DISRUPTIONS IN IT TECHNOLOGIES

10.1. An employee of the Company who notices a cyber attack against the Company or has detected any virus in the Company's systems shall immediately notify the Company's Chief Technology Officer.

10.2. Upon receipt of the notification provided for in Clause 10.1 of the Plan, the Company's Chief Technology Officer shall immediately, but not later than within 2 hours, take the following actions:

10.2.1. shall assess the possible impact of a cyber attack and/or virus, the reasons for its occurrence and shall contact the IT service providers engaged by the Company;

10.2.2. shall take any further action necessary to restore the affected functions and/or services of the Company;

10.2.3. shall inform the Head of the Company about the received notification.

10.3. The Company's Chief Technology Officer, having performed the assessment provided for in Clause 10.2.1 of the Plan, shall also draw up a plan of measures that may be implemented in order to prevent similar types of cyber attacks or viruses in the future and shall submit this plan to the Company's Chief Executive Officer. If necessary, the Company's Chief Technology Officer and the Head of the Company shall also consult with IT service providers and specialists in order to develop and implement appropriate plans and measures.

10.4. In order to prevent cyber attacks or viruses, the Head of the Company, in consultation with the Company's Chief Technology Officer or external service providers, must ensure the implementation of the following preventive measures:

10.4.1. periodic training of the Company's employees on cyber security issues. This training should take place at least once a year. The Head of the Company may use cyber security specialists for training;

10.4.2. choose reliable and market-known IT service providers that would ensure the maximum protection of the Company's IT systems from cyber attacks and/or viruses;

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

10.5. The Company shall also apply the following preventive measures in order to prevent cyber attacks:

10.5.1. training of employees shall be focused on the types of cyber attacks, their recognition and detection capabilities, preventive actions used to prevent viruses, etc.;

10.5.2. shall ensure that the Company has all essential IT solutions that protect the Company from cyber attacks and/or viruses, including, but not limited to, firewalls, antivirus programs;

10.5.3. shall select reliable IT service providers and periodically perform security analysis of IT systems.

10.6. Among other things, the Company shall follow the following principles and security measures in all cases when using IT solutions:

10.6.1. **IP filtering.** The administrative (management) zones of the IT systems used by the Company may be accessed only with pre-confirmed IP addresses. For this purpose, the persons and access points to which access is granted shall be identified (e.g. access to only predefined workplace IP addresses using a virtual private network (VPN);

10.6.2. **Restricted access.** The Company shall not create opportunities to connect to the databases used by the Company from the outside. Only pre-approved persons and previously known locations may 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, shall operate with the help of an SSL (Secure Sockets Layer) certificate. The SSL certificate shall help encrypt the information sent between the Customer and the Platform server, among other things. Browsing and other actions performed on the Company's website shall be encrypted using an SSL certificate;

10.6.4. **Monitoring.** The Company's website shall have a system installed that could be used to monitor user logins (login/logout time and date), see actions performed by users (edited items, confirmations, instructions, payments);

10.6.5. **Passwords.** In order to protect against fraud and other operational risks, the Company's customers shall be required to increase the complexity of passwords, i.e. passwords must be complex, consisting of 8 characters or more, including uppercase and lowercase letters, numbers, and additional specific characters. Secondary password (two-factor authentication) technology shall also be used;

10.6.6. **Connection security.** Firewalls shall always be used to connect to the external network for the Company's employees and systems.

11. ANALYSIS OF THE IMPACT ON THE COMPANY'S OPERATIONS

11.1. In order to ensure proper management of the Company's business continuity, the Head of the Company shall also periodically perform an analysis of the impact of possible incidents on the Company's operations, during which the potential impact of the Company's disruptions on confidentiality, integrity and availability shall be assessed.

11.2. The operational impact analysis shall be based on both internal and external data that may be provided by third parties. During the analysis of the impact on operations, the Head of the Company shall also assess the importance of the identified and classified business functions, ancillary processes, third parties and information resources and their interdependencies.

11.3. The Head of the Company shall also ensure that, taking into account the analysis of the impact on operations, the Company has implemented appropriate information and communication technology systems that ensure proper prevention of disruptions in the Company's operations and/or individual functions.

11.4. The Head of the Company, taking into account the analysis of the impact on operations, shall also decide on the need to adjust this Plan, providing additional measures to minimise the risk of the Company experiencing any negative impact due to disruption of the Company's operations and/or individual functions. If necessary, the Head of the Company shall redefine the business functions, auxiliary processes and/or other relevant procedures in order to ensure business continuity.

12. FINAL PROVISIONS

12.1. This Plan shall be approved and/or amended by the order of the Head of the Company. Amendments to the Plan shall take effect on the date of the Company's order, unless otherwise specified in the respective order.

12.2. The Plan must be updated to take into account experience gained in managing incidents, identified new risks and/or threats, and organisational changes.

12.3. This Plan shall be published on the Platform.

12.4. All employees and shareholders of the Company must be acquainted with this Policy by signing.

12.5. The Head of the Company shall be responsible for periodic testing and updating of the Plan. The Plan shall be tested at least once a year.

12.6. The Annex to this Plan contains a list of contact persons with whom it is necessary to maintain contact immediately in the event of a specific disruption of the Company's operations. In the event of a change in the details of these contact persons/service providers, the Head of the Company shall immediately update the information provided in Plan 1.

12.7. This Plan must be signed by all employees and shareholders of the Company.

12.8. The Head of the Company shall be responsible for periodic testing and updating of the Plan. The Plan shall be tested at least once a year.

12.9. The Annex to this Plan contains a list of contact persons with whom it is necessary to maintain contact immediately in the event of a specific disruption of the Company's operations. In the event of a change in the details of these contact persons/service providers, the Head of the Company shall immediately update the information provided in Plan 1.

CONTACT PERSONS

Inability of an employee to perform functions:

Head of the Company:	Laimonas Noreika Tel. No. +37060064899 E-mail laimonas@heavyfinance.eu

Loss of premises

Emergency services:	**112** – General emergency telephone number **011** – Fire station **022** – Police **033** – Emergency medical aid
Owner of the premises (Birutės st. 18-1, Vilnius):	UAB Verslama Tel. No. +370 686 41 395 E-mail nerijus@dataworld.lt
IT and server maintenance:	UAB Creation Labs Tel. No. +370 677 98 187 E-mail liudas@creation.lt

Platform disruptions

IT service providers maintaining the platform:	UAB Creation Labs Tel. No. +370 677 98 187 E-mail liudas@creation.lt

Malfunctions of operations of service providers

Internet service providers:	Telia Lietuva, AB Tel. No. +37064181817 E-mail info@telia.lt
Payment service providers:	Paysera LT, UAB Tel. No. +37052071558 E-mail info@paysera.lt
Third party that transmits customer identity data	Paysera LT, UAB Tel. No. +37052071558 E-mail info@paysera.lt

Data loss

IT and server maintenance:	UAB Creation Labs Tel. No. +370 677 98 187 E-mail liudas@creation.lt

State institutions	State Data Protection Inspectorate (8 5) 271 28 04, (8 5) 279 1445 E-mail ada@ada.lt

FORM OF CONFIRMATION OF EMPLOYEES THAT THEY HAVE GOT ACQUAINTED WITH THE COMPANY'S BUSINESS CONTINUITY PLAN

I HAVE BECOME ACQUAINTED WITH THE ABOVE:

No.	Name, surname:	Position	Date	Signature