1. CONTENTS

This activity plan describes Iron Bridge´s (herein after referred to as “the Company”) business regarding the issuance of electronic money. Flowcharts that show the administrative processes that exist for the business of issuing electronic money are available as appendices.

The content of this business plan must be updated continuously to correctly describe the business conducted at any given time.

If the business plan or the Company´s internal rules for issuing electronic money undergo significant changes, information on such changes must be submitted to us as soon as possible.

2. BACKGROUND

The Company is a company that publishes electronic money in its operations in accordance with the Electronic Money Act.

Considering the above, this activity plan has been prepared in accordance with regulations and general guidelines for electronic money and registered issuers.

In addition to issuing electronic money, the Company provides related services as described in section 6 below.

At present, the Company operates in the Gibraltar office.

3. PURPOSE

The purpose of the business plan is to describe in detail how the business of issuing electronic money and related services is to be conducted.

4. RESPONSIBILITY FOR THE OPERATIONAL PLAN

It is the responsibility of The Company CEO (CEO) together with the Compliance Officer to annually assess and update the content of the business plan and present them to the Board.

The CEO is responsible for informing all concerned about the provisions of this business plan. The responsibility is to ensure that employees within the Company know the content. In addition to this, consultants, partners, and contractors who are affected by the business plan must also be informed about the content.

Follow-up and control of compliance with this business plan shall be carried out by the CEO, Compliance Officer, and the Internal Audit.

5. ORGANIZATION

The Board has overall responsibility for long-term planning (strategic development) and for operational activities. We will soon appoint a CEO.

The Board has decided that the Company´s CEO will be responsible for the operations with electronic money and related services. The Company´s CEO will thus ensure that the Company's financial operations comply with applicable laws and regulations.

The Company has set up three special functions to ensure that the Company always meets, monitors, and works preventively with requirements in accordance with laws and regulations that the business requires: central function manager, compliance function and risk function. The Company has employees in Gibraltar. The Board considers that the current organization is sufficient for the business to be conducted with good internal governance and control in accordance with current external regulations. However, the board must continuously reconsider the need for employees and expand the organization as the business grows.

The board must meet at least four times a year, considering the holiday period during the summer. At board meetings, the members shall prepare reviews in accordance with the division of work. Each board meeting shall also include a presentation and review of compliance, risk, and the respective areas of responsibility of the central function manager.

6. SAFETY

6.1 PROTECTION OF INFORMATION

To ensure that unauthorized persons do not have access to confidential information, the Company´s premises will be locked and equipped with alarm systems to prevent anyone from gaining access to the premises.

When an employee is connected to The Company's network, the employee is protected in several ways. The Company's clients and servers always have updated virus protection and instructions on security updates from IT suppliers are implemented continuously. All emails received or sent are checked for viruses, all internet traffic and all email communications are logged and saved. Working documents regarding all levels of operations from reports to board documents are stored in the Company's intranet. All telephone calls, incoming and outgoing, are automatically recorded for both mobile and office telephony.

The Company has the opportunity, when deemed necessary, to control the use of networks, systems, internal and communication via email and telephony. The purpose of such control may be to:

a) Prevent concrete danger to networks and systems, e.g., in the event of a virus or hacker attack.

b) Take measures in case of reasonable suspicion that the Company's network, system, hardware, or Internet connection is used to commit a crime or prevent such crime.

c) Take measures of reasonable suspicion of such disloyalty that may lead to liability for damages or constitute grounds for termination / dismissal, e.g., if the Company's network, system and / or internet are used to conduct competing activities or disseminate confidential information (customer data, trade secrets).

6.2 SAFETY POLICY

The Company shall conduct active security work in accordance with applicable laws, regulations, and financial inspection regulations as well as other relevant rules in each country. The purpose shall be to prevent damage to person, property, and information due to accident, improper handling, or crime. The safety work must be based on continuous analyzes and follow-up and result in justified protective measures in the form of safety installations, work routines and safety rules. The staff must undergo ongoing training that provides such knowledge that it can best prevent crime and other injuries and handle criminal situations that have arisen. The Company must report all crimes against Iron Bridge to the police, both external and internal. It is especially important that:

• protect staff in the performance of their duties
• protect values such as money,
• prevent unauthorized access to information and conditions about the Company´s customers and to sensitive information about the Company´s operations
• ensure that the security of data operations is at a high level to prevent intrusions or disruptions that make data unavailable when needed or quality deficiencies that lead to poorer decision-making
• prevent unauthorized access to the Company premises,
• prevent fire, burglary, theft, vandalism, and financial crime.

The Company´s internal networks and systems are protected by firewalls. The Company's web services and integrated applications with partners 'and customers' networks / systems take place through the Company's DMZ (Demilitarized Zone), which is part of the firewall. In this way, all contact with external traffic from customers and others takes place without access submitted to the Company's internal network.

The Company´s workplaces and headquarters are interconnected via the internet. Security and functionality are ensured, between the different locations, using so- called VPN tunnel. The tunnel is installed over dedicated lines where data is encrypted for communication to take place in a secure manner. All workplaces have a firewall that only allows VPN traffic between the Company's internal networks.

7. RULE COMPLIANCE

The compliance function must consist of one or more persons and be directly subordinate to the CEO. Our partner in Gibraltar is responsible for the compliance function. The Compliance Officer is responsible for ensuring that the compliance function fulfills the areas of responsibility set out in the instructions for the compliance function and is especially responsible for all reporting on compliance with regulations. Compliance Officers 'areas of responsibility also include critically reviewing and questioning decisions that affect The Company´s compliance risks. The Compliance Officer shall have an ongoing dialogue with the Board and the CEO on regulatory compliance issues.

The Board is ultimately responsible for ensuring that the Company has the necessary resources and necessary support for compliance with regulations to be observed in all parts of the organization. The Board is the only function within Iron Bridge that has the authority to appoint or dismiss the Compliance Officer. The Board shall deal with compliance issues at each

ordinary Board meeting and the Compliance Officer shall complete a report every two months on the operations' compliance with the internal regulations. If the Compliance Officer finds serious deficiencies in the Company's internal regulations or internal reporting, or if it is otherwise required due to a change in the external regulations. The external regulations refer to obligations that follow from statutes, legislations, ordinances, and regulations from authorities. The board shall then be notified and convened without delay. It is of particular importance that opportunities have been established for employees to report identified or feared violations of current internal and external regulations.

The Compliance function's work must be risk-based for the Compliance function's resources to be distributed in an efficient manner. The compliance function's work shall thereby be focused on the regulatory compliance risks in the business that may mean that The Company is unable to fulfill its obligations in accordance with the rules that apply to the issuance of electronic money.

The compliance function shall, at the beginning of each financial year, prepare a written annual plan which shall be appointed to the board and the CEO. The annual plan must be approved by the board. The annual plan shall be a guide for how the Compliance function shall conduct its work in the coming financial year and shall be based on the risk assessment that is to be performed at least annually.

The annual plan must account for:

• risk analysis and considerations,
• planned activities for the financial year,
• control and monitoring program for the financial year,
• training activities for employees for the financial year, and
• follow-up of previous annual plan.

The compliance function has the following main areas of responsibility:

• check and regularly assess whether the internal regulations relating to compliance are complied with and are appropriate and effective
• evaluate measures taken to address deficiencies in the Company compliance
• provide advice and support to employees for the purpose of the Company operating in accordance with the requirements of the external and internal regulations,
• inform and train employees about news or changes regarding the external regulations and / or the internal regulations,
• make recommendations to employees regarding compliance issues,
• assist management and the board in all contacts with authorities.

8. RISK MANAGEMENT AND RISK CONTROL

The risk function shall consist of a Risk Manager who shall be directly subordinate to the CEO. The Risk Manager is responsible for ensuring that the risk function fulfills the areas of responsibility set out in the risk management instructions and is especially responsible for all reporting relating to risk. Risk Manager's areas of responsibility also include critically reviewing and questioning decisions that affect the Company´s risk exposure. Risk Manager shall have an ongoing dialogue with the Board and the CEO on risk-related issues.

The board shall ensure that the risk function has the resources required as well as access to the information needed to be able to fulfill its tasks. Furthermore, the board must ensure that the risk function has staff with the required knowledge and the powers needed to be able to fulfill their tasks. The staff must have sufficient knowledge of both methods and routines for managing risks, as well as markets and services to be able to provide relevant and independent information, analyzes and expert opinions on the Company risks.

The risk function must have appropriate systems and support at its disposal. The work of the risk function shall focus on the risks in the business that may mean that The Company is unable to fulfill its obligations that apply to the issuance of electronic money.

The risk function has the following main areas of responsibility:

• implement the internal regulations relating to risk management,
• check that all major risks to which the Company is exposed or may be exposed, are identified, and managed by relevant business units within the Company.
• identify risks that arise because of deficiencies in the Company risk management
• check that each business unit within the Company can effectively monitor all risks relevant to the business
• on the one hand, control, analyze and report the Company risks and the development of risks that may arise because of changed conditions, and on the other hand risks arising from the degree of complexity of The Company legal structure,
• ensure that information about the Company risks is regularly submitted to the Board and regularly, but at least quarterly, report its assessment both in writing and orally to the Board
• in cases where the board, CEO or functions submit proposals or make decisions that cause the Company´s risks to increase significantly, the function must assess whether these are compatible with the Company´s decision-making and in connection with this ensure that decisions are made at the right level in the Company,
• in cases where the Company develops or changes its strategy, risk tolerance and risk-taking, the function shall provide the board or CEO with all relevant risk-related information, which can form the basis for decisions in these matters and assess the proposed risk strategy and make a recommendation before the board decides about this,
• check that the internal regulations for risk management are appropriate and effective and propose changes to these if necessary
• identify, control and report risks of errors in the Company´s assumptions and assessments that form the basis of the Company´s financial reporting
• prior to decisions on significant changes in existing services, markets, processes, IT systems or other significant changes in the Company Limited's business or organization, the risk function shall evaluate risks with these and evaluate how these may affect the Company´s weighted risk.

It is the responsibility of the Risk Manager to ensure that the function's resources are distributed in an efficient manner. Risk Manager for the preparation of a written annual plan at the beginning of each financial year. The annual plan must be submitted to the board and the CEO and must be approved by the board. The annual plan shall be a guide for how the risk function is to conduct its work in the coming financial year and shall be based on the risk assessment that is to be performed at least once a year.

The annual plan must account for:

- risk analysis and considerations,
- planned activities for the financial year,
- control and monitoring program for the financial year,
- training activities for employees and affiliated agents for the financial year, and
- follow-up of previous annual plan.

The risk function shall annually review and evaluate which resources are necessary for the risk function to be able to fulfill the areas of responsibility. The review and evaluation must be reported in the annual plan.

The Company instructions for the risk function show how the Company identifies, measures, controls, internally reports, and controls the risks that the electronic money business is associated with...

9. MEASURES AGAINST MONEY LAUNDERING AND TERRORISM FINANCING

The internal regulations regarding measures against money laundering and terrorist financing have been established based on the requirements of the Act on Measures against Money Laundering and Terrorist Financing, as well as the regulations and general advice on measures against money laundering and terrorist financing. The internal rules regarding money laundering consist of a risk assessment together with an instruction.

A risk-based approach is the basis for the risk assessment and the Company's instructions on measures against money laundering and terrorist financing. This means that risks and situations are assessed and handled differently, depending on the specific risks of money laundering.

The scope of measures, processes, and internal controls as well as the allocation of resources are thus adapted based on the risk in the specific situation. In accordance with the purpose behind a risk-based approach, proactivity has been considered. The intention is to achieve a flexible system to optimally reduce the risks of the business being used for money laundering. A risk-based approach is applied in the customer awareness process, when reviewing transactions and when determining the scope and arrangement of internal control, including employee training and the scope of functions such as compliance, risk control and independent auditing (internal audit). Relevant requirements have mainly been considered in the design of the risk assessment.

The Company´s employees are expected to have or will have a developed knowledge and awareness of current issues based on their daily work, but it is of great importance that the board and the central function manager not only rely on the individual's knowledge and abilities but on an overall way develops instructions with routines that fully consider the requirements of the law. It makes it easier for the staff to work based on these routines in a service-wise and proactive manner and thereby ensure both business and complete compliance with regulations. It should be an overall purpose of the instructions and routines to eliminate as far as possible doubts and room for discretion for the staff and instead set clear and easy-to-follow requirements for the daily work.

10. CENTRAL FUNCTIONAL MANAGER

The central function manager is responsible to the board for money laundering issues within the business. The central function officer shall ensure that the Company instructions for money laundering and terrorist financing are reviewed at least annually and, if necessary, updated. In such a review, the Central Function Manager shall also review the effectiveness of the routines, measures, methods, and the like that follow from the instructions. If there is a need for updates to the instructions, the Central Function Manager shall prepare and propose written proposals to the Board.

The Central Functional Officer is also responsible for examining actual transactions to be able to detect such transactions that he suspects or has reasonable grounds to suspect form part of money laundering or terrorist financing or are otherwise deemed to be prohibited.

The central function manager must also establish control mechanisms, train staff, and create reporting opportunities regarding money laundering. The central function manager must also ensure that all employees take part in the Company´s instructions regarding money laundering and terrorist financing. Reporting regarding inspections and employee compliance shall be ongoing to the Board.

Furthermore, it appears from the employee's employment relationship that deficiencies in their compliance with money laundering can be both criminal and grounds for termination of employment.

11. EDUCATION PLAN

The Company's instructions on measures against money laundering and terrorist financing contain a training plan for money laundering. The teducation must be held by the Central Function Officer.

IRON BRIDGE LTD
Company number: 121007

Address:
5.20 World trade Center
6 Bayside Road
Gibraltar GX11 1AA