RULES
OF RISK MANAGEMENT IN TRADING ACTIVITIES
(INTERNATIONAL TRADING SYSTEM LIMITED)

1. General Provisions

1.1. These Rules of Risk Management for Trading Activities ("Rules") are an internal regulation of the International Trading System Limited ("ITS Ltd.", "Company") that establishes a combination of measures aimed to manage and mitigate risks that occur as the Company carries out its Qualified Investments trading, and when it combines trading activities with other types of activities. They create a regulatory basis for building an efficient risk management system, which corresponds to the nature and scope of the operations.

1.2. The Company risks means the possibility (probability) of the Company's loss as a result of adverse events connected with internal and/or external factors.

1.3. The Company establishes a risk management system in accordance with these Rules.

1.4. These Rules state the following:

- principles of organisation of the risk management system associated with the performance of the trading activity;
- goals and tasks of risk management associated with the performance of the Trading Operator activity, and when the trading activities combined with other types of activities.

1.5. These Rules:

- classify the risks typical for the Company;
- define the main methodological principles and approaches to identification, assessment, monitoring and control of the risks;
- establish the procedure and the timing for informing the Company's management bodies, Risk Management Department (RMD) and the Company's business units about the risks;
- establish the intervals for stress-testing of the trading tools and requirements to scenarios used for such testing;
- define measures aimed to manage uneconomic risks.

1.6. The Company updates the Rules by regular reviewing (at least once a year), and by amendments to them, if needed.

2. Risk management system associated with the performance of the trading activity

2.1. Risk management principles.

2.1.1. The risk management system of the Company is built on the following principles:

- ***The Worthiness principle*** means that the Board of Directors and the executive bodies of the Company should foster corporate culture based on reliable risk management, and support and create the adequate standards and incentives for responsible professional behaviour.
- ***The Comprehensiveness principle*** means that the sources of risk and objects of risk are identified based on comprehensive analysis of the existing and scheduled for introduction business processes and products, and the risk assessment and management procedures for the main activity of the Company are conducted in close connection with the risk management system in the areas not related to the main activity.
- ***The Involvement principle*** means that all the business units of the Company take part in the work of the risk management system. The Company's employees must immediately communicate to the line manager and the Risk Management Department («RMD») any information about the potential and committed violations of applicable laws, rules and internal regulations of the Company associated with the trading activities.
- ***The Continuity principle*** means that a required number of the orderly goal-oriented procedures, such as assessment of the actual risks, risk management system technology and operational regulations analysis and reporting to the management bodies, are implemented regularly.
- ***The Transparency principle*** means that the Company provides the stakeholders with the necessary information that describes the risk management system, including documents about the risk management system, risk assessment methodology and key aspects of the procedures for monitoring of the counterparty financial stability. At the same time, the results of evaluation of any specific counterparty expressed as ratings for internal use are not public information and may not be disclosed.
- ***The Assessment independence principle*** means that the comprehensive risk assessment and analysis are performed by separate business units/employees, independent from the units responsible for approving the risks and counterparties. The mentioned business units/employees may not

be tasked with duties, the fulfilment of which may lead to a conflict of interest.

- ***The Materiality principle*** means that the introduction of various elements of the risk management system must be based on the comparison of the costs of implementation of the analysis, control and management mechanisms with the potential benefits of the implementation, as well as with the cost of organisation and introduction of the products or services that carry the assessed risks.

2.2. **Goals and Tasks of Risk Management.**

2.2.1. The goal of the Company's risk management system is to limit and control the accepted risks in all areas of activity in accordance with own strategic tasks and goals, to ensure the sufficiency of own resources for covering the accepted risks, to increase the operational reliability and ensure duly running business processes of the Company, as well as keeping the Company's risks at a certain level.

2.2.2. The Company's risk management system includes processes and events designed to identify, analyse and assess the risks, treat the risks, monitor and control the Company's risks, and is aimed at the reduction of risks associated with the trading activities.

2.2.3. The goal of risk management is achieved based on systemic comprehensive approach, which ensures that the following issues are solved:

- classify and implement approaches to risk management accepted in the global practice;
- introduce an efficient risk management system at the Company, which helps to maintain the reliability of the activities aimed at Qualified Investments Trading and other types of activities, if the trading is combined with other activities, at a certain level and minimise loss due to the realisation of the risks;
- identify risk areas by determining the areas of the Company's activity subject to risks;
- identify risks by determining their sources and types of identified risks;
- analyse risks, in particular determine the risk measurement method, the probability of occurrence of such risks and the extent of their effect on the Company's activity;
- establish the allowed risk level and combined allowed risk level at the Company ("Risk limits");
- assess the risks by comparing their level to the maximum allowed risk level and combined allowed risk level set by the Company, to determine the method of treatment of such risk;
- treat the risk, which includes, in particular, a decision by the management bodies of the Company which will lead to risk avoidance, mitigation, acceptance or increase;
- monitor, review and control risks by assessing the risk changes and analysing the risk treatment results;
- exchange of information about the Company's risks between the Company's units, the Company's units and the Company's management bodies;
- Management bodies of the Company make strategically important decisions having full information about the risks, including about the probability of expenses (loss) and/or other adverse consequences of making any given decision.
- timely inform the Company's management bodies about the probability of occurrence and the extent of effect of a risk event, which would lead to expenses (losses) of the Company, about the level of realised risks and about the recommendations on how to mitigate or avoid such risks.
- control the execution of the decisions about the risk treatment measures taken by the management bodies, and the regular communication of information about the execution of the decisions to the Company's management bodies.
- provide conditions for seamless operation of the Company's software and hardware used for the trading activities.

2.3. **Authorities and functions of the management bodies of the Company, RMD and business units of the Company within the risk management system.**

2.3.1. The Company's management bodies must maintain corporate culture and ethical norms that demonstrate to all Company's employees the importance of risk management and promote risk awareness. Corporate culture and ethical values of the Company must in particular include the decisive value of timely and honest discussion of emerging problems. All the employees of the

Company, based on their authority and responsibilities, must be involved in the risk management activities and regard them as part of their job functions.

2.3.2. Any risk management includes:

- distribution of authority and functions in the risk management process of the Company between the Board of Directors and executive bodies;
- application of the main methods of risk control and/or minimisation by the business units of the Company (adoption of measures to keep the risk at the level that does not threaten the interests of the Trading Members, counterparties and the stability of the Company);
- submission of information about the risk events in the way prescribed by the regulatory documents, by the business units of the Company to the RMD;
- consistent exchange of information about the risks between the units of the Company in the aspects of risk management;
- immediate resolution of the emerging threats/risks;
- recording of the facts of the Company's risk occurrence and their treatment, and storage of the information used for risk management for at least 5 (five) years.

2.3.3. The competence of the Company's Board of Directors includes the determination of principles and approaches to the risk management system organisation, including, in particular, the following:

- identify the structure of the corporate governance of the Company;
- approve documents, make amendments (including the approval of a new revision), invalidate documents that establish the rules of the Company's risk management system organisation;
- approve, make amendments (including the approval of a new revision), invalidate a document that establishes the measures to be taken by the Company to restore financial stability;
- approve, make amendments (including the approval of a new revision), invalidate a document that establishes measures to be taken by the Company in emergency situations to ensure continuous activities aimed at Qualified Investments trading;
- determine the allowed level and combined allowed level for all the identified risk of the Company;
- check the actual state of the risk level for each of risk of the Company, and combined level of the risks of the Company, and control the observation of the allowed risk level and combined allowed risk level established by the Company by reviewing regular reports;
- control the execution of the risk control processes and events described in the Rules, in particular, analyse the information and control the execution of recommendations, by reviewing the quarterly reports about the state of the risks;
- control the risk management activity of the executive bodies of the Company.

The competence of the executive management of the Company includes tactical risk management, and, in particular, the following tasks:

- organise the development and introduction of internal regulations for the rules and procedures of the Company's risk management;
- ensure the approval of internal regulations that define the rules and procedures for the risk management;
- distribute authorities and responsibilities in the risk management sphere between the business units of the Company and the management staff, provide them with the necessary resources, establish the procedures of interaction, data exchange and reporting;
- control the execution of the risk management processes and events described in the Rules, analyse the information and control the execution of the recommendations obtained by reviewing the risk state reports and reports on the results of the trading tools stress-testing on the securities market;
- determine the allowed level and combined allowed level for all the identified risk of the Company;
- control the actual state of the risk level for each of the Company's risks, and the combined the Company's risk level, and control the execution of the Risk limits set by the Company;
- approve the action plan to mitigate or avoid significant risks of the Company in case of exceeding the allowed risk level.

2.3.4. The day-to-day the Company's risk management is performed by RMD and the Company's employees within their competence. The head of the RMD is the Director of RMD.

2.3.5. RMD may not perform any functions that are not related to the risk management and execution of internal control, except for some cases described herein.

2.3.6. RMD is independent of other officers and business units of the Company in the execution of its duties.

2.3.7. RMD may not be assigned responsibilities, the fulfilment of which may cause conflict of interest, and the Director of RMD may not execute functions associated with the performance of operations and the conclusion of transactions of the Company.

2.3.8. The RMD employees may be included in the committees and commissions created by the Company, which are not the business units of the Company.

2.3.9. The competence of RMD includes:

- training (consulting) for employees of the Company on the matters of risk identification, assessment and mitigation.
- analyse and predict the state of the risk management system, to identify the critical (most unsafe) business processes and sources of risk, to evaluate the capital adequacy, financial resources and reserves for risk management;
- identify and investigate potential threats and vulnerabilities of the Company, plan prevention measures;
- develop methods and tools of risk management;
- collect and analyse internal and external data associated with the risks of the Company, detect risk concentration points and determine the reasons of their occurrence;
- assess the risks of the Company considering the probability of occurrence and impact on the Qualified Investments Trading;
- develop guidelines for the management bodies and heads of the Company's business units about the measures to eliminate any given risk for the Company;
- control the implementation of measures aimed to minimise the identified the Company's risks;
- provide the information about the Company's risks to the Company's management bodies by means of regular reporting;
- communicate to the employees of the Company the information required for the Company's risk mitigation;
- take part in the developing of the documents that regulate the activity of a Trading Operator;
- within their authority: take measures to ensure the confidentiality of information obtained in the process of the Company's risk management, within the framework of the data collection, analysis and storage;
- take other measures aimed to manage the risks mentioned in the internal regulations of the Company.

2.3.10. RMD must have resources and authority required to perform its functions, including:

- access to all information systems (in view mode) and internal regulations of the Company, which may affect the risks of the Company;
- right to demand additional information from the management and employees of the Company (including information in written form) in connection with the performance of risk management obligations;
- right to immediately response to the day-to-day activities of the Company in the order prescribed in the internal regulations of the Company;
- right to take part in the meetings with the participation of the Company's Board of Directors, dedicated to the discussion of issues related to the risks of the Company, with the right to submit questions for discussion, and in the work of the part-time risk management bodies: task teams, dedicated committees, etc.;
- right of RMD Director to directly discuss the risk issues with the Senior Executive Officer of the Company.

2.3.11. All the business units of the Company must consider the risk management aspects within their authority, coordinate their activity with the RMD, interact and exchange information with RMD on all the issues connected with the risk management sphere. In order to ensure effective performance of the risk management system, the interaction between the business units of the

Company and the RMD may be initiated by any of the parties in the ordinary course of business. If necessary, the issues related to risk management in the activity of a business unit may be submitted for review of the Company's management bodies.

2.3.12. Performing their functions, the business units must observe the established rules, procedures and technologies.

2.3.13. For the risk management, the most important factors are:

- following the procedures that ensure the Company's business continuity;
- provision of the measures that preserve the business reputation of the Company;
- observing of the set limits and restrictions for the handled operations;
- meeting the requirements to the asset composition and structure;
- control over the flow of funds;
- securing of the future payments;
- correspondence of the assets and liabilities on the balance sheet in terms of the completion times;
- observing of the applicable legal requirements about the securities market
- monitoring of changes with the right to regulate the securities market, to search for unaccounted risks;
- observing of the established order of access to information and documents;
- distribution of the rights of access to information resources and provision of information security;
- identification of the Trading Members and counterparties;
- registration, confirmation and recording of the Trading Member orders;
- timely and full consideration of appeals, applications and claims of the Trading Members;
- timely and quality preparation of reports;
- identification and timely settlement of internal conflicts between the employees and between the employees and the Company;
- informing of the new employees about the corporate culture of the Company, accepted ethical norms and principles of risk management;
- timely settlement of the claims to the Company (its employees).

2.4. **Requirements to the day-to-day management of the Company in connection with the risk management**

2.4.1. The Company's Board of Directors and the management bodies of the Company are responsible for the organisation of the duly corporate governance. The corporate governance structure must ensure the creation of an effective control environment.

2.4.2. For the creation of the Company's corporate governance structure, internal rules and technologies, taking into consideration the established corporate culture, the Company adheres to the following norms:

- avoid duplication (partial duplication) of the authority of the Company's business units, ensure clear delimitation of the job duties, their strict observance and enforce of accountability at all levels;
- exclude the possibilities for excessive internal and external influence of the interested parties on the Company's unit employees and the business decision-making, limit the concentration of authority, ensure correspondence of the scope of authority and responsibility of the business units, the Company's control bodies, managers and employees, introduction of the formalised collective decision-making procedures;
- eliminate any possibility to perform both executive and control functions for the Company's units, managers and employees of the units of the Company;
- ensure control over the technology elements of the business processes and contacts with the Trading Members and counterparties depending on the level of potential risks, eliminate the potential for uncontrolled operations and contacts associated with the exchange of any type of information available to the Company, which is not public knowledge and contains details about the Company and Trading Members, and the information about the Trading Members operations, which gives an advantage to persons possessing such information due to their job title, employment duties or an agreement made with a Trading Member compared to other parties to business relationships ("Internal Use information");
- segregation of duties of the Company's employees, fragmentation of business processes,

procedures and technology into elements so that a single unit, or a management staff representative, or an employee may not perform (control) them entirely from the beginning to the end.

3. Main risks associated with the activity of the Company

3.1. The Company performs continuous identification of risks arising in the process of the trading activities or when the Company combines the trading activities with other types of activities. Risk identification involves comprehensive analysis of the external and internal conditions of the Company's operation in search of potential for the occurrence of risk factors.

3.2. As part of the management of the risks of consequences that result in the suspension or termination of Qualified Investments Trading services in full or in part, the Company has determined the following types of risks:

3.3. **Operational risk** means a risk of expenses (loss) as a result of faults and/or errors of the software and hardware systems of the Company, including software and hardware and information and telecommunication systems, which are used in Qualified Investments Trading, and/or in the internal business processes of the Company, mistakes of the employees and/or as a result of external events that have negative effect on the trading activity.

3.4. **Market risk** means a risk of expenses (loss) due to an adverse change in the market value of financial instruments or other assets, in which the funds of the Company are invested.

3.5. **Regulatory risk** means a risk of expenses (loss) and/or other adverse consequences due to the non-compliance of the activity performed based on the licence of the Trading Operator, to the requirements of AIFC Regulations and Rules, rules of Qualified Investments Trading, founding and other documents of the Company and/or as a result of measures against the Company by AFSA.

The Internal Control Department of the Company is responsible for the identification, analysis, assessment, monitoring and control of regulatory risk of the trading activity, as well as its management.

3.6. **Credit risk** means a risk of the expenses or loss of the Company due to failure to perform, untimely or incomplete performance of contractual financial obligations to the Company by a counterparty.

4. Main approaches to risk identification, assessment, monitoring and control.

4.1. **Operational Risk.**

4.1.1. To manage the operational risk, the Company:

- determines the procedure and methods of identification, assessment, monitoring, control and/or minimisation of the operational risk;
- takes other measures mentioned herein to manage the Company's operational risk.

4.1.2. An operational risk occurs as a result of:

- suboptimal, insufficient and/or inefficient control procedures in systems and processes;
- inadequate acts of employees (including mistakes, internal frauds);
- imperfections of the organisational structure and internal regulations in the aspect of the distribution of authority of the units and employees, practices and procedures of operations, their recording and accounting recognition;
- failure of the employees to follow the established practices and procedures;
- inefficiency of internal control;
- faults in the system and equipment operation;
- adverse external factors out of the Company's control (including external fraud, man-made and natural disasters).

4.1.3. The operational risk identification process includes the analysis of all the conditions of the Company's operations for the presence or potential for occurrence of the operational risk factors, which must be conducted at several levels:

- analysis of external information;
- analysis of the susceptibility to operational risk in the Company's business areas;
- analysis of internal procedures and business processes;
- analysis of internal structural changes;
- analysis of individual operations.

4.1.4. To identify, monitor and assess the operational risks, and to determine the actual state of the trading tools, their operational reliability and effectiveness for handling increased load, in particular, to check whether the trading tools need to be updated, the Company arranges regular stress-testing of the software and hardware (load testing) used for the trading activities.

4.1.5. The list of processes, suspension of which leads to the disruption of the normal business activity of the Company, its counterparties and/or Trading Members, including the threat of the full loss of their operating resource ("Critical processes", "Important services"), is established by the Company in the Business continuity plan.

4.1.6. The software and hardware of the Company, which presents the risk of suspension or termination of the provision of Critical processes in full or in part and/or other negative effect on the activity of the Company in case of faults and/or errors in their operation, includes the following:

- Prospective trading and clearing system (PTCS) is a computer program enabling organisation and carrying out of Qualified Investments Trading of the financial instruments;
- Servers, other equipment used for the functioning of PTCS.

4.1.7. In case of detection of deficiencies in the operation of the trading tools, revealed as a result of test operations (testing) of the trading tools and/or based on the information received by RMD from the heads of the Company's business units about the identified lack of correspondence between the software and hardware and the nature and scope of operations performed by the Company, the RMD includes the details on such deficiencies in the regular reports, and provides recommendations on the resolution of deficiencies in the trading tools, and also, if necessary, recommendations on the improvement (update) of the software and hardware.

4.1.8. The Company provides the right to use software required for participation in the Qualified Investments Trading, to a Trading Member, and the Trading Member must in turn have the technical capacity to participate in the Qualified Investments Trading.

4.1.9. The Company sets the requirements to the software and hardware used by the Trading Members and their clients for the connection to the trading tools, and also discloses such requirements on the Company's website on the Internet.

At the time of arranging the connection to the trading tools, the Trading Members may consult with the Company's specialists who provide technical support to the Trading Members.

4.1.10. The Company provides to Trading Members/counterparties a possibility to contact the Company's technical assistance administration in case of errors/drawbacks in the operation of the software and hardware affecting their participation in Qualified Investments Trading. Appeals of the Trading Members/counterparties to the Technical assistance administration may be sent by e-mail or by phone, using contact details provided on the website of the Company. Employees responsible for the interaction with the Trading Members/counterparties on the matters of the provision of technical access to trading, verify the information about the Trading Members/counterparties finding errors in the work of the software and hardware, and, if such errors are confirmed, record the appeals of the Trading Members/counterparties and eliminate the found deficiencies, notifying the Applicant of the task completion. The Technical assistance administration of the Company must communicate the information about the detection of errors and deficiencies in the work of software and hardware to RMD.

4.2. **Market risk.**

4.2.1. The market risk occurs as a result of revaluation loss of the market value of financial instruments or assets, in which the Company's funds are invested.

4.2.2. To reduce the market risk, the Company:

- limits the list of vehicles, in which the funds of the Company may be invested;
- sets the list of allowed investment vehicles, in which the funds of the Company may be invested;
- regularly monitors the investment Portfolio Value of the Company.

4.3. **Credit risk**

4.3.1. The source of the credit risk is a possible failure to perform the obligations to the Company in the process of investment activity performed by the Company by one or several counterparties.

4.3.2. In order to limit the credit risk, the Company:

- conducts a preliminary comprehensive analysis of the financial status of counterparties;
- limits the list of vehicles, in which the funds of the Company may be invested;
- determines the list of allowed investment vehicles for the process of investment activity of the Company;
- regularly monitors the financial status of the counterparties.

4.4. **Risk analysis, risk assessment and determination of the risk treatment measures**

4.4.1. The Company performs risk analysis, which includes determination of the method to measure the risks according to quality and quantity assessment criteria.

4.4.2. The Company applies various methods of risk assessment, including the following:

- direct assessment;
- assessment by key indicators;
- expert evaluation.

4.4.3. In general, the risk analysis and the risk level assessment are conducted based on the probability of their occurrence and possible financial consequences for the Company's activities. The results of the risk assessment are communicated to the control bodies of the Company by means of including in the regular reports.

4.4.4. By the decision of the Company's management bodies, measures against the risk may be taken. The Company may take a decision aimed to avoid, mitigate, accept or increase the risk.

4.4.5. The actual risk assessment is compared with the established the Company's Risk limits. If the allowed risk level is exceeded, the Company classifies such risks (except for operational risks) as significant.

4.4.6. With regard to the risks that are classified as significant by the Company, the Risk Management Department shall develop an action plan to mitigate or eliminate significant risks of the Company. The action plan is subject to approval by the Senior Executive Officer of the Company. The action plan must be reviewed if new significant risks or additional facts are identified, which require the development and implementation of the measures to remedy the identified violations of the Risk limits and/or other measures with regard to the risks of the Company in order to mitigate or eliminate the Company's risks.

4.4.7. The information about the implementation of the action plan is also communicated to the Company's management bodies in the regular reports of the Company.

4.5. **Risk Monitoring and Control**

4.5.1. To ensure the environment for effective monitoring and control of the operational risk events, the Company maintains an analytical database ("ADB"), which contains the information about all of the identified operational risk events and includes the following data:

- type of risk;
- date of the realisation of the Company's risk event, which has led or may lead to expenses (loss) of the Company;
- description of the risk event;
- circumstance of the occurrence (identification) of the Company's risk event;
- amount of expenses (loss) incurred by the Company due to the realisation of the risk event;
- measures taken by the Company to eliminate the identified violations;
- Risk Management Department recommendations to reduce the identified risks;
- indication on the significance of the risk event;
- other information (if necessary).

4.5.2. Material events are those operational risk events that cause suspension or termination of the critical processes of the Company, including extraordinary events.

4.5.3. The information of the ADB is entered by the Risk Management Department employees as the relevant events are identified and the control measures with regard to the operational risk created

due to such events are taken, no longer that on the work day following the date of identification/obtaining of the necessary data from the business units.

4.5.4. The risk level monitoring is performed based on the analysis of the collected data about the facts of occurrence/change of the Company's risks.

4.5.5. The information about the change of the risk level obtained in the process of risk monitoring is communicated to the management bodies of the Company, business units and employees whose activities may be affected by the change of the risk level.

4.5.6. To control the risks, the Company's sets the Risk limits and monitors whether the identified risks are within the Risk limits. The Company regularly prepares reports for the Company's management bodies to be submitted at the intervals and in the time and reflecting the information about the actual state of the risks.

5. Measures taken by the Company to ensure confidentiality and protect internal use information about the Company's risks and the information provided by the Company to the service provider.

5.1. The information about the Company's risks is classified as Internal Use and to the full extent is subject to protection procedures applied to such type of information.

5.2. To ensure the confidentiality of risk-related information, including the confidentiality of risk reports of the Risk Management Department, the following procedure for information and report provision in the risk management sphere, to the Company's employees, Board of Directors and the Company's management bodies.

- In the course of operations aimed to identify, assess, monitor and control the risks, the Risk Management Department informs the employees of the Company's business units about the identified risks assigned to the authority of their respective business units, in the amount necessary to ensure effective contributions of the employees to risk assessment and creation of the action plans to mitigate and/or control the risks.

Unless otherwise determined in the internal regulations of the Company:

- the timing of informing the business unit employees and submission of reports to the Company's business units is determined by the Risk Management Department based on their professional judgement taking into consideration the risk assessment;
- the timing and form of the provision of information by the Company's employees to the Risk Management Department are stated in a corresponding Risk Management Department request.
- the Company's management bodies shall have complete and up-to-date information from the Risk Management Department, including risk reports, observing the timing and the procedure established in these Rules.

5.3. To ensure information confidentiality and protection, (including the information provided by the Company to the service provider), the Company takes the following actions:

5.4. ***Organisational measures:***

- information confidentiality requirements are set in all cases in the service provision agreements between the provider and the Company;
- security procedures to restrict access of unauthorised persons to the Company premises, including access to hardware located on the premises;
- the Company has specialised security and video surveillance systems are in place to avoid unauthorised access to the premises;
- access to technical areas with the IT-equipment (server equipment) shall be granted only to those the Company's employees who are required to work with such hardware (equipment) because of their official duties.

5.5. ***Technical controls:***

5.5.1. In order to protect the Internal Use information from unauthorised access when it is transmitted via open communication channels, the following cryptographic tools are used:

- digital signature (handwritten signature equivalent) to protect the Information from unauthorised modifications;
- data encryption to protect from unauthorised disclosure of the Information to third persons;
- a system of delimitation of access is in place for the Information storage and processing at work

stations and servers, which allows giving access to the Information only to authorised the Company's employees and prevent unauthorised access by other employees and unauthorised persons.

6. Procedure for development and approval of the Business continuity plan

6.1. Considering the risk of abnormal and emergency situations, the Company prepares and updates a Business continuity plan, which establishes the coals, tasks, procedure, methods and timing for the implementation of measures to prevent and timely remedy the consequences of a possible disruption of the day-to-day operation mode due to abnormal situations.

6.2. Business continuity plan is developed for abnormal situations comparable to a municipal emergency situation in terms of duration and impact, scale of possible financial losses and negative non-financial consequences.

6.3. The business continuity plan is approved by the Board of Directors of the Company.

6.4. Preventive revision (update) of the Business continuity plan is carried out at least once a year in order to check sufficiency of measures provisioned to ensure trading activities continuity, correspondence of measures provisioned in the Plan to actual conditions of Business continuity plan implementation and current requirements, as well as its correspondence to the organisational structure, nature, and scale of the Company's activities and the Company's development strategy.

6.5. Business continuity plan is subject to complete revision in following cases:

- in case of material changes in the list of tasks and/or configuration of software and hardware of information systems causing significant changes in information processing technology;
- in case of changes in priorities of threats for information system security;
- if insufficiency of action plans to ensure the Company's business continuity is identified based on the nature of the Company's activities and volume of operations being performed;
- in case of material changes in requirements of legislation pertaining to the Company's business continuity.

6.6. Business continuity plan is subject to partial revision in following cases:

- in case of material changes in configuration, adding or removal of software and hardware of information systems, that do not change information processing technology;
- in case of changes in configuration of software and hardware, that do not change information processing technology;
- in case of material changes in the list, duties, and authorities of system users.

6.7. In order to define the possibility of the Business continuity plan implementation in case of occurrence of Abnormal situations, the Business continuity plan checking (testing) with the simulation of potential Emergency situations and involvement of the Company's employees is carried out at the intervals established in the Business continuity plan.

7. List of circumstances that may lead to the suspension or termination of the provision of important services.

7.1. The Company's ensures continuous process of identification of the circumstances and situations, which may lead to the suspension or termination of the Critical processes, as well as affect the business activities.

7.2. At the same time, the Company considers a possibility of the occurrence of circumstances that cause and/or create preconditions for failures in operation of a hardware and software system and/or immediately hindering its normal (standard) functioning (in particular, force majeure events, as well as equipment failures, faults, and troubles; software errors; failures, faults, and troubles of communication systems, power supply, conditioning, and other life support systems, as well as other conditions, such as violation of access control rules and/or attempts of unauthorised access to computer systems, abnormal situations of smaller scale, including those connected with the manifestation of the following factors (separately or in combination) ("abnormal situation"):

- hardware failures, failures of information systems (in particular, as a result of technical failure) used to serve Critical processes;
- disturbance of utility infrastructure (flooding of the Company's premises, e. g. due to a pipe break, etc.);
- failures in power supply (in particular due to refusal of power suppliers to fulfil their obligations),

that cannot be eliminated using hardware available to the Company;

- violation of communication channel operation (in particular due to a technical failure and/or refusal of communication channel supplier to fulfil their obligations).

Other circumstances, which may, as decided by the Company, lead to the suspension or termination of the Critical processes:

- the Company receives a message from a clearing centre about an emergency situation, which may lead to a disruption of service for Trading Members;
- an attempt by third persons to get unauthorised access to protected information, or intentional creation of conditions that hinder the regular operation of the software and hardware at the Company (network attacks);
- adoption of or any amendments to the AIFC Regulations and Rules, as well as instructions, guidelines, statements, letters, telegrams or other actions of the relevant state authorities, which have made, are making or may make the further continuation of the activity, as well as the provision of other important services in the form and order, in which such operations were performed before the adoption of such regulations, impossible or very difficult.

8. Measures taken by the Company in emergency situations and directed to ensure the continuity of the trading activities

8.1. In case of an emergency situation the Company does the following:

8.1.1. using all the available means of communication, immediately informs the Clearing Organisation that provides clearing services to the Company and is mentioned in the Rules of Qualified Investments Trading, about the occurrence of an abnormal situation that may lead or has led to a violation in the provision of services to a Trading Member/Trading Members;

8.1.2. using all the available means of communication, immediately informs the Trading Member/Trading Members, a supervisory authority and other persons about the occurrence of an emergency situation;

8.1.3. in case of a violation of service provision to a Trading Member/Trading Members, the decision about the trading suspension shall be made by the Senior Executive Officer according to instructions in the Business continuity plan;

8.1.4. if necessary, a Crisis team is created by the decision of the Senior Executive Officer as described in the Business continuity plan,

8.2. To settle an emergency situation, the Company may take (if necessary, subject to coordination with the Clearing Organisation), in particular, the following measures:

- change the end time of the trade session, during which the emergency situation has occurred;
- change the timing and procedure of document flow in the process of interaction between the Company and the Clearing Organisation;
- conduct an additional trading session;
- implementation of other actions aimed at resolving the emergency situation.

8.3. The decisions taken to resolve the emergency situation are binding on all Trading Members.

8.4. The Trading Members, the Clearing Organisation, AFSA and other stakeholders are notified of the measures taken to resolve the emergency situation by the available means of communication no later than the day of taking these measures.

9. Measures to ensure seamless operation of the Company software and hardware used for the trading activities

9.1. Measures to ensure the seamless operation of the Company's software and hardware and other equipment required for hardware operation and communication channels ("Equipment"):

- use failsafe hardware for the Equipment, to ensure the backup of the main server equipment subsystems, data storage systems (by configuring hard drives as failsafe RAIDs), which will help to avoid Equipment downtime in case of a failure of single server equipment components and/or single components of the server equipment data storage systems;
- ensure the availability of the sufficient transmitting capacity of the communication links and communication equipment, as well as sufficiently fast response of the software and hardware of the information systems, and the possibility to expand them to process increasing volume of operations

during peak load;

- establish a combination of measures to monitor the increase of load on the software and hardware of the Company and avoid the exceedingly high volume of the incoming applications from the Trading Members, and their frequency;
- install and operate the Equipment in a technologically advanced room, use highly reliable production resources to ensure the Equipment operation;
- ensure the connection of the server hardware to the Internet using communication links with two independent failsafe 24-hour communication channels, and adopt measures to ensure continuous availability of production resources, communication links, control of the condition of the production resources and equipment;
- promptly adopt measures to replace the components of the Equipment out of service in case of hardware failures in the Equipment components, as part of scheduled and preventive maintenance.

9.2. Measures to ensure continuous operation of the software set ("Software"):

- use reliable high-quality software with the adequate reliability, failure safety, efficiency, availability, scalability and maintenance efficiency characteristics;
- configure the software to ensure the balance of load on the server equipment components and, where possible, the possibility to continue to run the software without downtime in case of a single component failure;
- perform automatic and regular manual control of the software operation, automated monitoring of the key parameters of the software condition for early detection of potential issues in the operation of the system-wide software and application software, automatic notification to System Administrator about the potential for the issues based on the results of the software condition parameter monitoring.
- monitor the intensity of the software use by Trading Members;
- ensure continuous availability of the software System Administrator for timely response in case of detection of potential problems or functional failures of the software and its components;
- use the information protection tools to ensure the protection from unauthorised access to the Software by means of software features, preventing data modification, tampering with the regular Software operation mode, trading processes;
- adopt measures to protect the Software from network attacks, including possible measures for automated detection and elimination of attacks, use the Software security analysis tools and network safety monitoring tools.

10. Procedure for the distribution of responsibilities and authorities between the business units of the Company and their employees in case of occurrence of material operational risk events and/or identification of emergency situations

10.1. Whenever an event that leads to an interruption of the Company's activity or a drop in its service level ("incident") is detected:

10.2. An employee having witnessed the incident immediately contacts the head of their unit, who makes a decision on the incident significance and the Company's unit ability to continue operations.

10.3. A head of the Company's business unit:

- estimates current situation, possible consequences, and the main reasons to the fullest extent possible;
- if necessary, notifies a corresponding emergency service;
- makes a decision about the significance of the event and about the ability of the business unit to continue operation in regular mode, and about the extent, to which the incident affects the operation of other units, and communicates this information to the Senior Executive Officer of the Company (officer performing the duties of the Senior Executive Officer of the Company);
- informs the Company's units or the persons responsible, whose performance of duties is essential for maintaining the Company's activities.

10.4. The Senior Executive Officer of the Company (officer performing the duties of the Senior Executive Officer of the Company) makes decisions to minimise the consequences of the identified incident.

10.5. If needed, the Senior Executive Officer (officer performing the duties of the Senior Executive Officer) makes a decision about the commencement of operations in emergency regime (acknowledge an emergency).

10.6. Once decision is made to commence operations in emergency regime (acknowledge an emergency), operations are carried out under one of crisis Business continuity plans.

11. Measures taken by the Company to protect the information and documents related to the organisation of Qualified Investments Trading

11.1. In the trading activities, the Company uses the following mechanisms and methods for the protection of information and documents related to the organisation of on-exchange trading:

- protection of information in the access management and registration processes;
- protection of information at the stages of the Life Cycle of automated systems;
- protection of information by antivirus tools;
- protection of information during the use of resources of the information and telecommunication network Internet;
- provision of the security and control procedures (encryption, encoding, protection from unauthorised access during the information transfer and storage, software that restricts access to data, authentication and authorisation of the members);
- protection of information in the process of assigning and distributing roles;
- organisation of work of the Information Security Administration;
- management of the information protection violation risks;
- regulation and documentation of activities that ensure the information protection, including the procedure for registration and information storage;
- increasing of awareness of the employees in the area of the information protection;
- detection of the Information Security Incidents and response to them;
- monitoring and analysis of the provision of information protection;
- timely improvements of the protection of information.
- long-term planning for the information and computer systems, specification of requirements to them, vendor selection and supervision of the projects aiming create systems and technology for data processing and transmission for the Company;
- provision of the staff access only to the data required to fulfil their direct official duties within the given authority;
- access restriction by taking advantage of the software features;
- provision of the systems for delimitation of access to different levels of databases and operational environment at the local network level;
- installation of the Company's property items in the premises with access control mode;
- provision of the continuous operation procedures for the software and hardware of the Company used to perform trading activities, including:
- fully redundant architecture of the computer system, without the non-redundant points of failure, immune to non-repeated hardware failures in any type of components, which can ensure the functioning of the main electronic systems used by the Company;
- provision of a continuously updated action plan for situations when the backup facilities and components of the computer centre must be used, and regular drilling of the measures prescribed in that plan;
- operability recovery and return to normal operation procedure for disrupted internal processes and systems;
- provision of the project solutions integrated in the application systems, which ensure the load distribution and mutual backup at the access server level and main data processing servers;
- use of high-availability clusters with integrated redundancy of the main components as a platform the most critical tasks;
- use of telecommunication devices with redundant main units in standard configuration;
- use of the fully redundant architecture storage devices for databases and other critical information;

- provision and unfailing implementation of procedures for regular (at least once a day) backup of all critical data, which implies storage and regular update of backup copies;
- provision of redundant versatile workplaces;
- provision of a computer centre for the automatic fire-fighting system in the premises;
- 24-hour monitoring of the state of computing and telecommunication equipment and premises of the computer centre of the Company;
- redistribution of functions, authorities and responsibilities of the units and employees;
- measures to maintain adequate information supply, assessment preparedness to emergency situation with regard to information service providers.

11.2. A delimitation of access system is in place at the work stations and servers for the storage and processing of information and documents associated with the organisation of trading, which ensures access to data only to authorised employees and prevents unauthorised access by all the other employees and outsiders. This system works both at the level of the system and network facilities and in the applications used by the Company.

11.3. The Company's has established, implemented, recorded and monitored the rules and procedures of monitoring the access to information, analysis and storage of data about the employee actions and operations, which allows identifying unauthorised or suspicious operations.

11.4. The Company's has implemented the logs of actions and operations for automated workplaces, server and network equipment, firewalls, to use them in response to incidents with the information and documents.

11.5. Information monitoring procedures and actions and operations data analysis procedures use recorded criteria for the identification of unauthorised or suspicious activities and operations. The mentioned monitoring and analysis procedures are applied regularly to all the completed actions and operations.

11.6. The Information security administration of the Company is responsible for the protection and control of the access to information.

12. Procedure for risk management effectiveness assessment and risk reporting.

12.1. Within the risk management activities, the risk management performance is assessed at least once a year, by analysing the effectiveness of the detection of the Risk limit violations, their resolution and/or measures to mitigate or avoid the risks.

12.2. The Company's risk management system effectiveness is assessed by the Company's Board of Directors based on the following information:

- information about the achieved level of risks and observing of the set risk limits;
- information about the amount of loss incurred by the Company as part of the trading activities;
- reports of the Internal Audit Department about the results of the performance check of the risk management check.

12.3. The Internal Audit Department, in accordance with the work plan approved by the Board of Directors, performs an audit of the organisation and performance of the risk management system associated with the trading activities, including the performance assessment in terms of following the internal regulations of the Company, which determine the requirements to the risk management system, and then provides a report about the audit results to the Board of Directors.

12.4. After the end of the reporting year, the Director of RMD analyses the entirety of data about the risks and assesses the effectiveness of the risk management system by checking against the criteria that determine the effectiveness of the risk management system. The results of the assessment may be included in the current quarterly Report on the state of the risk management system, or in a separate report on the effectiveness of the risk management system, and submitted for review by the management bodies of the Company.

12.5. Based on the analysis of the results of the previous calendar year, the Company's Board of Directors gives an assessment of performance of the risk management system.

12.6. The risk management system is considered effective if it meets the following criteria:

- no significant (and/or above) loss resulting from the trading activities, which affects the financial stability of the Company;

- the established risk limits are observed;
- timely stress-testing of the software and hardware for the Company's Qualified Investments is ensured;
- risk mitigation measures are in place;
- recommendations of the Internal Audit and Internal Control Departments are put into practice in timely manner.

12.7. If the results of the risk management system performance assessment are unsatisfactory, the Board of Directors makes decisions aimed to resolve the identified problems and bring the risk management system in line with the nature and scale of the activities of the Company.

12.8. Within its competence, the Company's Board of Directors may decide to develop (improve) the risk management system based on the strategic tasks of the Company considering the international and domestic experience in the risk management sphere and other external and internal factors that may affect the quality of the risk management.

12.9. In order to ensure effective risk management, the main principles and approached to the risk management are reviewed and updated by the RMD as needed as part of the Rules of Risk Management for Trading Activities.

12.10. The Director of RMD ensures the preparation of the following reports on the risks of the Company:

- quarterly report on the status of the risk management system;
- report on the violation identified.

12.11. Quarterly report on the state of the risk management system includes an analytical part, including an interpretation of the obtained results and recommendations regarding the measures of risk management, and in particular containing:

- Risk assessment and Risk level justification in the main areas of the Company's activities;
- details on the facts of loss, violations and exceeding of the Risk limits;
- details about the causes and results of investigating the facts of loss, violations and exceeding of the Risk limits;
- measures taken to remedy the detected violations and mitigate the risks;
- details on the RMD recommendations on the risk mitigation/elimination;
- details on the fulfilment of the RMD recommendations on the identified risk mitigation/elimination;
- details on the fulfilment of the Action plan intended to mitigate significant risks of the Company or avoid them (if any significant risks are identified and the Action plan to mitigate the significant risks of the Company or avoid them, is prepared);
- details about the detection of deficiencies in the trading tools operation, and on the inadequacy of the software and hardware for the nature and scope of operations performed by the Company, identified as a result of the trading tool testing;
- details about the fulfilment of recommendations on the resolution of deficiencies in the trading tool operation and, if needed, recommendations to improve (update) the software and hardware;
- other information about the Risks, which the RMD Director may deem necessary to provide.

The quarterly report is created and submitted for review to the Company's Board of Directors, the Company's Management committee and the Senior Executive Officer of the Company, no later than 30 (thirty) days from the end of another quarter.

12.12. The report on the violation identified is formed in case of identification of risk events with high losses as well as a significant excess of Risk Limits due to the implementation of risk events.

12.13. A report on the identified violation includes:

- details of the identified violation;
- measures to eliminate the identified violation;

12.14. The Report on the identified violation is submitted to the Senior Executive Officer of the Company, the Company's Management committee and, at the discretion of the RMD Director, to the heads of the Company's business units no later than 10 (ten) work days from the date of identification of the relevant violation.

13. Final Provisions

13.1. The requirements set forth in these Rules are mandatory for all the employees of all Company's business units.

13.2. RMD employees may demand from the employees and officers of the Company to provide information (documents), including written explanations, on the issues arising in the course of their performance of their duties.

13.3. Persons who violate or fail to follow the requirements of these Rules, are subject to disciplinary or administrative measures.

13.4. The heads of the Company's business units are personally responsible for the fulfilment of duties by their subordinates.

13.5. These Rules are subject to the approval of the Company's Board of Directors.

13.6. If the AIFC Regulations and Rules are modified, or amendments are made to internal regulations of the Company, then the parts of the Rules that do not contradict such changes should be valid until the Rules are harmonised with the changes.