APPROVED

by the resolution of the Supervisory Board

of the Moscow Exchange

on 26 February, 2018, Minutes # 13

POLICY

on Information Security Management

# of Public Joint-Stock Company Moscow Exchange MICEX-RTS

Moscow 2018

TABLE OF CONTENTS

LIST OF AMENDMENTS

Version	Approval date	Description
1	31.07.2015	Approval of the first version by the Supervisory Board of the Moscow Exchange
2	26.02.2018	Approval of the second version by the Supervisory Board of the Moscow Exchange

1. General Provisions

1.1. This Policy on Information Security Management (hereinafter referred to as the Policy) shall be a fundamental document of the information security system of the Moscow Exchange (hereinafter referred to as the Company), setting the priorities, principles and methods of ensuring information security amid threats characteristic of and material to the systems and information technologies of the Company.

1.2. Requirements herein shall supplement those of the Company’s Declaration on Information Security and consider the requirements of the information security legislation of the Russian Federation, international standard on information security ISO/IEC27001:2013, the current status of and immediate prospects for the development of the Company’s information infrastructure, as well as capabilities of today’s organisational and technical methods of information protection.

1.3. The requirements of this Policy and other internal documents for ensuring information security shall be binding upon all Company employees.

1.4. All derogations from the requirements of this Policy and other internal documents related to information security should be documented and agreed upon with the Department of Operational Risks, Information Security and Business Continuity. Attachment A contains the form of documenting derogations from the IS requirements.

1.5. The Information Security Management System (hereinafter referred to as the ISMS) is part of the Company-wide management system based on the assessment of information security (hereinafter referred to as IS) risks and designed to develop, implement, maintain, monitor, analyse, support and improve IS.

1.6. The Glossary section contains main terms and definitions used herein.

2. Glossary

ISO/IEC 27001:2013 (Standard) – International Standard “Information Technology – Security Techniques – Information Security Management Systems – Requirements”.

P$_{threat}$ – probability of threat occurrence.

Administrator of the information system (IT Administrator) – a Company employee responsible for administering a certain information system (IT system).

Backup Administrator – an employee of the Information Technology Unit, who is responsible for performing backup procedures. Backup Administrator may be assigned to one or several Company IT systems.

Asset – anything of value to the Company and at its disposal.

Update – monitoring and analysis of the effective internal documents of the Company, as well as amendments made thereto if necessary.

Antivirus software (AVS) – software designed to detect and eliminate malicious software.

CWS – a computer work station.

ISMS auditor – a Company employee whose functions include regular and comprehensive review of ISMS compliance with the requirements of the Company’s normative IS documentation and the Standard.

Business Owner of a risk – a Company employee at least of the Department Director level, who is responsible for the impact of an identified risk, as well as for making decisions on its treatment technique (accept, avoid, transfer, mitigate).

Asset Owner – a structural Company unit represented by its head, which is primarily responsible for managing and monitoring the use of an asset and ensuring the security of the asset (an information system, process, etc.), as well as for determining the severity of impact of an IS threat occurrence on the assets they own.

Owner of an information system – a senior Company employee assigned to each information system and responsible for decision-making on matters within his remit in accordance with the normative documents of the Company’s IS management system.

Owner of a confidential information medium – a unit responsible for storing and maintaining such a medium.

Risk Owner – a Company employee responsible for implementing measures in accordance with the decision made on the risk treatment technique.

Making changes – a modification, including the implementation, update and decommissioning of information infrastructure elements, which affects the Company’s information assets.

External party – a Company partner, supplier, client or any other person or organisation the Company has dealings with in its business operations except for Moscow Exchange Group companies.

Malicious software – software capable of violating the Company’s information security.

DCS – the Department of Corporate Systems in the Information Technology Unit of the Moscow Exchange.

Documentation – the defined process of recording information on a hard copy, which results in producing an official document approved by the organisation management.

DORIS&BC – the Department of Operational Risks, Information Security and Business Continuity.

Accessibility – the property of providing information to the authorised user, with its type and place required by the user and at a time when they need it.

MD – the Maintenance Department of the Information Technology Unit of the Moscow Exchange.

Life Cycle (LC) – the combination of interrelated processes of building and consistently modifying the state of an information infrastructure facility ranging from developing its initial requirements to ending its operations and scrapping the complex of automation tools.

Record – a document containing achieved results and evidence of performed activity.

Change to access rights – provision or withdrawal of access rights.

Inventory check – the process of identifying and documenting assets which are of value to the Company and at its disposal.

Information Security (IS) – security related to threats in the sphere of information.

Information infrastructure (IT infrastructure) – the total of systems for information processing and processed data, which is used to ensure Company operations.

Information system (IT system) – a system consisting of the total of interrelated hardware and software automation tools to implement the information technology of performing Company functions.

Information asset – software, hardware system or software and hardware system performing required functions within the Company's business process.

IS incident – a one-off undesirable and unexpected IS event (or the total of such events) which may threaten IS (violate the confidentiality, integrity or accessibility of Company information).

Classification of information assets – breakdown of the Company information assets into types, which is done according to the criticality of their significance to the achievement of the Company's business goals.

Emergency Management Team (EMT) – a collegial body of the Company authorized to coordinate the actions of the Company units and individual employees in case of emergency as part of the body's assigned authority in accordance with their job descriptions and provisions of the Business Continuity Policy.

Committee on Information Security and Business Continuity (IS and BC Committee) – a consultative and advisory body of the Company's executive authorities, which pursues its activities in order to prevent and/or minimise damage (direct or consequential, material or other) done to the parties of information relations by undesirable impact on information, its media and data handling processes, as well as damage resulting from potential impact of external and internal events which may entail a partial or full suspension of the operations of the Company and/or NSD and/or NCC Clearing Bank.

Company – the Moscow Exchange.

Equipment compromise – a fact of unauthorised access to equipment, as well as suspicion of attempting such an access.

Password compromise – loss of guarantee that the password is known only to authorised persons.

Confidential information – electronic (digital) information processed in the Company's information infrastructure, as well as its hard copy or otherwise, the access to which is limited in accordance with the applicable legislation of the Russian Federation. The Company's confidential information includes commercial, official secret, as well as personal data and other secrets protected by law.

Confidentiality – an information property of being inaccessible and otherwise not disclosed to unauthorised users.

Cryptographic key (key information) – secret information used by the CIPF in coding/decoding messages, creating and checking electronic signature and calculating authentication codes.

Sponsor of information security (IS sponsor) – the Director of the Department of Operational Risks, Information Security and Business Continuity.

License key – a file containing data confirming license availability for a certain period of time required for proper work of antivirus software.

Local Area Network (LAN) – the total of servers, computer work stations and peripheral equipment which function in a single information environment created through organising their interaction by means of telecommunications equipment.

Business Continuity Manager – a Company employee whose functions include coordination of actions to ensure the Company's continuous activities and fail-free functioning of the Company’s business processes.

Information Security Manager (IS Manager) – a Company employee responsible for the coordination of activity to implement, operate, control and maintain the Company’s ISMS at a proper level.

IS Training Manager – a Company employee whose functions include the organisation, planning and regular holding of IS training courses, including the organisation of the training process and testing of employees’ IS knowledge.

IS Risk Manager – a Company employee responsible for making a comprehensive ISMS analysis and developing recommendations on the improvement of management mechanisms.

Incident Manager – a Company employee whose functions include the organisation of and support for a set of actions to prevent and respond to IS incidents, as well as managing the accumulation of information about IS incidents.

ISMS Methodologist – a Company employee responsible for managing the processes of development, implementation and review of ISMS-related normative documents.

Metric of ISMS process efficiency (Metric) – a digital value that makes it possible to determine an ISMS performance indicator.

Mobile device – a portable device used to store, process and transfer information (e.g. a laptop).

Access rights monitoring – checking the conformance of released user access rights to those actually installed in information systems.

Account monitoring – checking the relevance of accounts existing in IS.

Information medium – a material object capable of storing (carrying) for a sufficiently long time the information recorded on/in it.

ISMS scope – the totality of processes, information assets and elements of the Company’s information infrastructure.

Inventory sphere – limits of an inventory check, which may include one or several business processes of the Company.

Security upgrades (Upgrades) – software upgrades whose absence may cause a breach to the confidentiality, integrity or accessibility of information processed by IS.

Information infrastructure object (IIO) – software, a technical device, their complex or an information system used by the Company in processing and transfer of digital information.

Company facility – premises, a building or a building compound which houses the components of the Company's information infrastructure.

Object of information asset environment – a material object of the environment using and (or) maintaining an information asset (object of storage, transfer, processing, protection, etc.).

Residual risk – the risk remaining after risk treatment.

IS risk assessment – description of identified IS risks, determination of such characteristics as probability of threat occurrence (threat probability) and severity of impact (SI)

List of Unit's standard software – a list of names and versions of software solutions used by most users in the unit.

Raising awareness – a regular process of training and raising the level of practical and theoretical skills of employees and representatives of external parties by using various methods and tools.

ISMS performance indicator – the value which is received after a math transformation of relevant metrics and makes it possible to determine the performance of the information security management system.

Document users – a group of Company employees to whom the normative document is addressed, who take part in the process regulated by a normative document and are guided by its provisions.

User – a Company employee or a representative of an external party, who uses Company information systems.

Privileged user – a user who has administrative authority with respect to IS.

Note: The management system includes an organisational structure, policies, development of plans, responsibility distribution, instructions, procedures, processes and resources.

Software (SW) – the total of programs and software packages to ensure the operations of CA and area networks.

Scanning mode – the process of information verification launched automatically or manually by a Company employee and aimed at detecting malicious software.

Risk – a measure considering the potential possibility of using the vulnerabilities of an asset or a group of assets to do damage to the Company. It is determined using a combination of terms of threat probability and the cost of loss (damage) resulting from the occurrence of this threat.

Information Security Risk (IS Risk) – a risk related to the possibility of losing IS properties (confidentiality, integrity, accessibility) of Company information assets as a result of IS threat occurrence. It is determined by the probability of threat occurrence (threat probability) and the extent of severity of impact (SI).

Head of the IS Systems Testing Group – a Company employee whose functions include the organisation and holding of actions to assess the robustness of applied protection techniques and tools.

Head of the IS Infrastructure Maintenance Group – a Company employee whose functions include support/backup, monitoring and setting of information security tools.

Public domain software – software whose use does not require the acquisition of any rights.

Signature bases – data bases used in antivirus software and containing the description of all malicious codes (viruses) known at present to the software developer, as well as the techniques of their removal.

System of information antivirus protection (AVP system) – a set of organisational actions, technical and software tools designed to ensure protection of Company information infrastructure from threat posed by viruses and other malicious software, as well as from spam propagation.

Information Security Management System (ISMS) – part of the general system of Company management based on IS risk assessment and designed to develop, implement, operate, monitor, analyse, support and improve information security.

Computer aid (CA) – the total of software and technical elements of data processing systems capable of functioning on their own or as part of other systems.

Information security tool (IST) – technical, software and software technical tools, substance and (or) material designed or used for information security.

Cryptographic Information Protection Facility (CIPF) – the total of software and hardware tools ensuring the implementation of the following functions: creation/verification of electronic signature, coding/decoding of electronic documents and e-messages, creation of public and private (secret) keys of electronic signatures and encryption, cryptographic transformation of information to ensure its confidentiality and integrity.

SI – severity of impact of violating properties of information assets. Depending on the information asset properties, it can be SI of confidentiality breach, SI of integrity breach, SI of accessibility breach.

Structural unit – officially assigned part of the Company and its employees performing the established range of duties and responsible for meeting their assigned objectives.

Threat – danger suggestive of a potential loss (damage).

Information Security threat – a threat of violating the IS properties (accessibility, integrity, confidentiality) of Company information assets.

IS risk management – a continuous, cyclical and documented process of identifying, collecting, using and analysing information which allows the assessment of IS risks.

Damage – a loss, contingency costs, loss of property or opportunity loss, resulting from unfavourable impact on Company business (loss of assets, damage (loss of properties) to assets and (or) to infrastructure of the Company).

Functional requirement – formalised user requirement for implementing a new information system software or modifying the existing one.

Integrity – information stability in the process of its transfer or storage.

Soft copy – an information medium designed to record and store data and based on any physical effect that enables the system to have two or more stable states.

3. Company business context

3.1. Understanding the Company and its business context.

3.1.1. The Company is the biggest organiser of trade in the commodities and financial markets in Russia and it provides Russian and foreign investors, professional financial market participants and their clients a wide range of opportunities to trade shares, bonds, fund units, derivatives, currency, government securities and commodities.

3.1.2. On the platform of the Company's Equity & Bond market, encompassing sections of the Equity & Bond market, REPO market and deposit market, holds shares, federal loan bonds, regional and corporate bonds, sovereign and corporate Eurobonds, depositary receipts, investment units, mortgage participation certificates and exchange trade funds trading; provides management services for execution of REPO transactions with CCP, inter-dealer REPO transactions, direct REPO transactions with the Bank of Russia, as well as operations regulated by the Bank of Russia, the Pension Fund of Russia, the Federal Treasury of Russia, Vnesheconombank, etc.

3.1.3. The Company's derivatives market trades index futures contracts (MOEX Index, RTS Index, RVI Index); Russian and foreign equity futures, federal loan bonds and Eurobonds Russia-30, currency pairs, interest rates; commodity futures contracts (gold, silver, platinum, palladium, copper); crude oil and sugar futures; option contracts for some of these futures.

3.1.4. The Company's currency market trades currency pairs of the following currencies: US dollar (USD), euro (EUR), Chinese yuan (CNY), British pound (GBP), Hong Kong dollar (HKD), Ukrainian hryvnia (UAH), Kazakhstani tenge (KZT) and Belarusian Rouble (BYR). The most actively traded currency pairs are USD/RUB and EUR/RUB.

3.1.5. The Company also offers its clients information and technological services. In the course of rendering information services both market data in real time and information on trade results and indexes are provided.

3.1.6. The Company actively promotes the Russian financial market and its infrastructure, improves technologies and increases attractiveness of its trade management services in the commodities and financial markets for local and foreign investors and issuers.

3.2. Understanding needs and expectations of stakeholders.

3.2.1. Out of necessity to manage trading at regulated markets, the Company exercises its best efforts to identify needs and expectations of all its stakeholders.

3.2.2. The Company's stakeholders include:

- the Central Bank of the Russian Federation;
- other government and legislative bodies that regulate the Company’s activity;
- Moscow Exchange Group affiliated companies;
- current and potential investors including shareholders;
- market participants, market data users;
- internal users – employees of corporate units interacting in the ordinary course of business;
- key service providers.

3.2.3. The requirements of all the stakeholders are being constantly monitored and analysed to sustain the Company’s ongoing activities. For the purpose of the Company development planning it is the stakeholders’ needs that provide the basis for changes implementation and functionality development as well as introduction of new services.

3.3. Opportunities.

3.3.1. The Company enjoys the following opportunities ensuring achievement of expected results for the information security management system:

- competent and informed staff receiving periodical professional training;
- a relevant infrastructure, including data processing centres, is defined, secured and maintained;
- high transparency of the Company’s activities in compliance with the actual corporate governance standards is ensured;
- the Corporate Governance Code complies with the best international practices.

4. Concept, Goals and Objectives of Information Security

4.1. Information security is taken to mean protection of information and its processing equipment from accidental or deliberate impact whether natural or artificial.

4.2. The main goal of ensuring IS shall be to achieve appropriate protection of Company business processes, as well as to minimise IS risks in organising trading, clearing services, providing services on the stock, derivatives, FX and money markets.

4.3. The said goal shall be achieved by ensuring and continuously maintaining the confidentiality, integrity and accessibility of the Company’s protected information assets.

4.4. To achieve the main IS goal, the Company shall ensure effective solutions to the following objectives:

- make an inventory and classify the Company’s information assets;
- identify IS risks and opportunities;
- establish and improve the information security management system, including the processes of IS assessment and analysis;
- determine and document basic IS requirements and procedures;
- implement and set information security tools;
- train Company personnel in the IS sphere;
- timely detect and remove vulnerabilities of Company assets and by so doing prevent any possibilities of damage and disruption caused to the normal operations of Company business processes by IS threat occurrence;
- reduce potential Company damage to an acceptable level in case of IS threat occurrence, including shorter time of resumption of business processes following potential interruptions;
- plan and optimise Company IS costs.

5. Principles of Information Security

5.1. The main principles of ensuring the Company's information security shall be:

5.1.1. *Compliance* – application of IS measures and techniques in strict compliance with the provisions of applicable IS legislation of the Russian Federation.

5.1.2. *Consistency* – consideration of all interrelated, interacting and time-varying elements, conditions and factors, which are meaningful to Company IS.

5.1.3. *Comprehensiveness* – coordinated application of heterogeneous tools to build an integral security system that blocks all essential channels of IS threat occurrence without any weaknesses in those places where some of its components interface.

5.1.4. *Multi-level protection* – use of several security barriers to IS threat occurrence.

5.1.5. *Continuous protection* – IS activity shall be an integral part of the Company's day-to-day operations and must not be interrupted, including constant support for physical, technical and software resources, as well as continuous control over execution of IS requirements.

5.1.6. *Timeliness* – the Company should timely detect IS threats potentially capable of impacting on the achievement of Company business goals, forecast potential ways of their development, assess the extent of their influence on business processes and apply IS measures where and when they are necessary.

5.1.7. *Adequacy* – applied IS measures should be effective and proportionate to existing IS risks with due account of the cost of such measures and the size of potential losses resulting from the occurrence of threats.

5.1.8. *Feasibility* – all the IS requirements should be realistic, attainable and non-conflicting.

5.1.9. *Continuity and improvement* – continuous improvement of protection measures and tools on the basis of continuity of organisational and technical solutions and of personnel.

5.1.10. *Flexibility* – the Company ISMS must be able to respond to changes in external environment and conditions for the Company to do its business.

5.1.11. *User-friendliness* – ISMS building and update should consider and wherever possible to minimise potential problems for users to work with security tools and to execute main IS procedures.

5.1.12. *Documented approach* – all IS requirements and measures, as well as the outcome of IS activities should be documented.

5.1.13. *Awareness of IS requirements* – all Company employees should know the amount of IS requirements corresponding to their job descriptions and access to Company information resources, as well as be guided by them in their work.

5.1.14. *Minimisation of authority* – Company employees shall be granted access only to those information assets and only t the extent, which is required to execute their job duties.

5.1.15. *Exclusion of conflict of interest* – a clear division of responsibilities and exclusion of such situations where the scope of employees' responsibilities allows for a conflict of interest. In particular, none of Company employees should be authorised to single-handedly perform critical operations.

5.1.16. *Knowledge of own clients and employees* – the Company should be informed about its clients, carefully select employees and servicing staff, develop and maintain corporate ethics by creating a favourable trusted operating environment for the Company's management of information assets.

5.1.17. *Personal responsibility* – each Company employee within their authority shall be responsible for compliance with the IS requirements.

6. Organisation of Information Security Management System (ISMS)

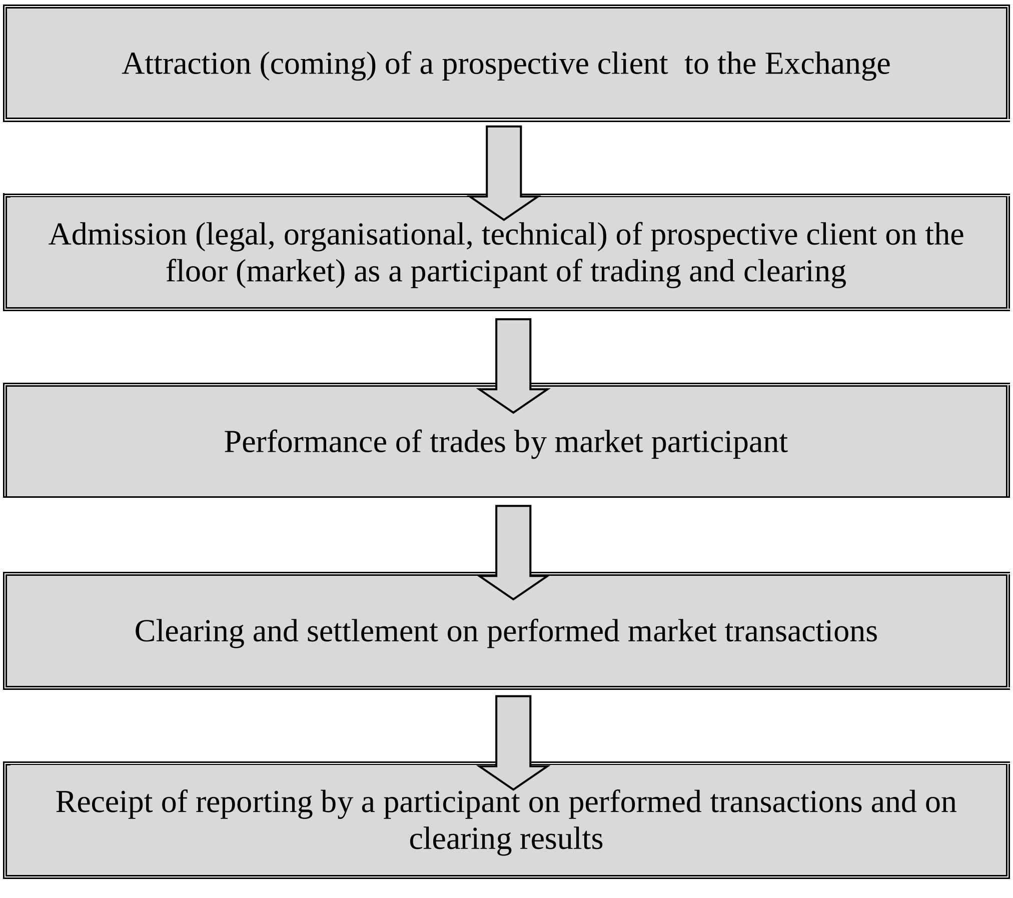
6.1. **ISMS Definition**

6.1.1. The ISMS constitutes a part of the overall system of Company management, is based on IS risk assessment and designed to develop, implement, operate, monitor, analyse, support and improve information security in the Company.

6.1.2. The management system shall include an organisational structure, policies, plan development, responsibility distribution, instructions, procedures, processes and resources.

6.2. **ISMS Scope**

6.2.1. The ISMS scope shall be Company business processes related to organisation of trading, clearing services and provision of services on the stock, derivatives, FX and money markets and shall cover the following single technological chain:


Attraction (coming) of a prospective client to the Exchange
Admission (legal, organisational, technical) of prospective client on the floor (market) as a participant of trading and clearing
Performance of trades by market participant
Clearing and settlement on performed market transactions
Receipt of reporting by a participant on performed transactions and on clearing results

6.2.2. The ISMS scope shall cover the following structural units of the Company:

- basic units implementing the technological chain of organising trading, clearing services and service provisions on the stock, derivatives, FX and money markets:
    - the Operations Department

- auxiliary units providing the technological chain for organising trading, clearing services and service provisions on the stock, derivatives, FX and money markets:
  - the Department of Corporate Systems
  - the Department of Trading and Auxiliary Systems Support
  - the Maintenance Department
  - the Technical Support Division
  - the Security Department
  - the Client Support Department
  - the Department of Operational Risks, Information Security and Business Continuity
  - the Personnel and HR Policy Department
  - the Document Management Division
  - the Procurement Management Division

6.2.3. The ISMS scope shall also include all information assets owned and (or) processed by the Company, including confidential and public (openly accessible) information. These assets shall implement and support the operations of such a technological chain.

6.2.4. The following offices of the Exchange fall within the scope of the Business Continuity Management System:

Office 1: 125009 Moscow, Bolshoy Kislovsky per, 13
Office 2: 125009 Moscow, Vozdvizhenka Str, 4/7, Bld 1

6.2.5. The Company shall properly protect IS properties (confidentiality, integrity, accessibility) of information assets at each level of the IT infrastructure hierarchy. At the same time, ensuring IS properties for an information asset shall include setting up a required protection of its matching environment objects by reducing or fully blocking this object's vulnerabilities through using protection measures.

6.2.6. The main objects of the Company's IT infrastructure, which are subject to protection shall be:

- information assets required for Company operations irrespective of their form and kind;

– IT infrastructure elements, including information technologies, hardware and software resources for creating, processing, transferring, storing (including archiving) and using information, including libraries, archives, databases, information exchange and telecommunications channels, information security systems and resources, facilities and premises housing protected elements of Company IT infrastructure;

– processes, regulations and procedures for information processing in the Company;

– Company employees.

6.3. **ISMS Execution**

6.3.1. The Company ISMS shall be executed and operated on the basis of a process approach. For IS execution and maintenance the Company shall employ four process groups:

– ISMS planning (planning);

– ISMS execution (execution);

– ISMS monitoring and analysis (verification);

– ISMS support and improvement (improvement).

6.3.2. The groups of the Company ISMS processes shall be organised as a cyclical model of "planning – execution – verification – improvement – planning – ...", which provides the basis for the Company's ISMS model.

6.3.3. The Planning Stage shall include the development of IS policy, activity to determine the ISMS scope and IS risk assessment, selection and development of plans to implement protective measures (including IS risk treatment plans).

6.3.4. The Execution Stage shall include the implementation of all plans related to ISMS building, installation, improvement, and to the implementation of protective measures. Among other things the Company shall execute activity in training and raising the awareness of personnel in the IS sphere, detecting IS incident and responding thereto, as well as ensuring Company business continuity.

6.3.5. The Verification Stage shall include compliance checks of selected protective measures against established IS requirements, as well as assessment of the Company's IS compliance with the requirements of RF legislation, the Standard and Company internal documents.

6.3.6. At the Verification Stage the result of the performed activity shall provide the basis for ISMS improvement, which includes decision-making on implementing corrective and preventive measures. At the same time, ISMS shall be improved as part of the Execution Stage and if necessary − the Planning Stage.

6.3.7. Mindful of the IS importance, the Company Management shall initiate, support, analyse and control the implementation of ISMS processes that promote conditions for further business development with acceptable risks.

7. Areas of ISMS Development and Improvement

7.1. **Focal Areas of ISMS Development and Improvement**

7.1.1. This Policy shall define the following focal areas of continuous ISMS development and improvement:

– distribution of functions and responsibilities between Company employees in the information security sphere;

– management of ISMS documentation;

– management of information security risks;

– monitoring and analysis of ISMS performance and improvement of the ISMS processes;

– ensuring information security while working with personnel;

– raising the level of IS awareness among Company employees and increasing IS awareness control;

– work with third parties;

– ensuring physical security and equipment protection;

– technical and organisational measures to ensure information security;

– management of Company IS;

– management of information security incidents;

– management of business continuity;

– compliance with legislative requirements;

– use of licensed software;

– internal audits of information security.

7.1.2. The requirements hereof should be detailed in appropriate individual policies, regulations, procedures, provisions, instructions and methods developed within the ISMS.

7.2. **Distribution of Roles and Responsibilities in Information Security**

7.2.1. In order to execute, operate, monitor and maintain the ISMS at a proper level, the Company within the Department of Operational Risks, Information Security and Business Continuity has created the following areas of activity led by the head of each area:

- information security,
- business continuity;
- operational risks.

7.2.2. The employees of the Department of Operational Risks, Information Security and Business Continuity within their remit shall organise and control the execution of all Company IS actions to reduce IS risks and manage them, shall organise ISMS establishment and operations, as well as IS maintenance in accordance with the requirements set by the ISMS.

7.2.3. The Director of the Department of Operational Risks, Information Security and Business Continuity shall plan costs and allocate resources, including finance, required to execute and operate ISMS and manage risks on the basis on action plans of each of the above Department activity areas represented by their heads. Planning may also involve other Company units if necessary.

7.2.4. Relevant IT Unit structural units jointly with the Department of Operational Risks, Information Security and Business Continuity shall execute technical IS actions and delimit access to Company information assets.

7.2.5. The Director of the Department of Operational Risks, Information Security and Business Continuity shall sponsor the activities of the above Department areas in order to maintain interrelation of IS goals with those of the core business operations of the Company, to raise IS awareness levels and involve the Company Management in ISMS operations.

7.2.6. The Information Security and Business Continuity Committee has been established to coordinate the Company's information security business. The Committee shall be the central body of planning, organising and controlling the execution of this Policy.

7.2.7. Additionally, as part of the ISMS, it is necessary to determine employees responsible for performing the following roles:

– *Information Security Manager*, who is responsible for coordinating activities related to implementation, operation, control and proper maintenance of the ISMS across the Company.

– *Business Continuity System Manager,* who is responsible for managing the Company business continuity system and ensuring continuous functions of Company business processes;

– *Incident Manager*, who is responsible for organising and supporting a complex of measures to prevent IS incidents and respond to them, as well as for investigating IS incidents;

– *IS Risk Manager*, who is responsible for analysing the ISMS and developing recommendations for improvement of management tools;

– *ISMS Auditor*, who is responsible for regular comprehensive assessment of ISMS compliance with the requirements of the Company's normative IS documentation and the Standard;

– *ISMS Training Manager,* who is responsible for organisation, planning and regular holding of IS training, including organisation of the training process and testing of employees' IS knowledge.

– *ISMS Methodologist*, who is responsible for developing, analysing, monitoring and updating normative IS documentation, as well as for ensuring ISMS document workflow and record management.

7.3. **ISMS Documentation Management**

7.3.1. The development, execution, agreement, registration, storage, transfer and destruction of documentation related to the Company ISMS should meet the document management requirements approved by the Company.

7.3.2. All ISMS documentation should be safeguarded. Access to documentation both in hard and soft copies and containing confidential information should be limited and granted only to those Company employees who need them to fulfil their job duties.

7.4. All provisions of the Company's IS documentation should be in agreement and conform to the requirements of this Policy.

7.4.1. The process of ISMS operations should include the creation of records to determine ISMS compliance with approved information security requirements, as well as to analyse its performance for further improvement.

7.4.2. The copies of effective internal documents and records related to Company ISMS should be stored in the Department of Operational Risks, Information Security and Business Continuity.

7.5. **Risk Management**

7.5.1. To develop an effective ISMS, achieve appropriate protection of Company information assets and their respective environment objects, the Company shall execute IS risk management activities, which is an integral part of the entire IS Company activities and is applied both during ISMS implementation and its current operations.

7.5.2. IS risk management shall constitute a continuous process involving the analysis of what may occur, as well as potential consequences followed by decision-making on what should be done and at what time in order to mitigate risks to an acceptable level by preventing IS threats and (or) by minimising impact in case of a risk event.

7.5.3. The approach to IS risk management should be harmonised with the overall approach to risk management of the Company's core activity and corresponds to the Company's operating environment.

7.5.4. The risk assessment procedure and methodology shall be defined and documented. It is necessary to determine responsibility for IS risk development and review, as well as for the approval of risk acceptance criteria and residual risk level. Reviewing risk assessment outcome at planned intervals, including the review of residual risks and established levels of acceptable risk, shall be mandatory.

7.5.5. Information security measures should aim to identify IS risks effectively and timely where and when such measures are necessary.

7.6. **Monitoring, Performance Analysis and Improvement of ISMS Processes**

7.6.1. The Company should monitor the ISMS processes in order to:

– promptly identify errors in information processing results;

– promptly identify successful and failed attempts of information security breaches and incidents;

– detect variances of the planned process of Company information security and determine the causes thereof;

– assess the performance of actions to improve the ISMS (by introducing special performance indicators – metrics).

7.6.2. The Company should regularly, at least once a year, analyse the ISMS. The procedure should consider the deliverables of security audits, statistics and additional information on occurred IS incidents, results of the performance evaluation of IS processes, as well as proposals and comments from all the stakeholders.

7.6.3. The Company should continuously improve the ISMS by applying corrective and preventive measures determined upon the results of ISMS analysis. The procedure for selecting, agreeing and applying corrective and preventive measures should be documented.

7.7. **Ensuring Information Security while Working with Personnel**

7.7.1. The Company should set IS requirements at the following stages of relations with employees:

– during recruitment;

– during the employment contract period;

– at the time of dismissal or transfer to another position.

7.7.2. The Company should conclude an employment agreement with each employee to set out mutual obligations and rights of the Company and employee. The employee must always sign a contractual commitment not to disclose confidential information, which defines their IS obligations towards the Company.

7.7.3. Upon dismissal or transfer to another position all employees should return the Company’s information assets provided to them for temporary use when they performed their job duties. The procedures for Company employees’ dismissals and transfers to other positions, for equipment return and cancellation (change) of access rights should be documented.

7.8. **Raising IS Awareness Levels of Company Employees and Increasing Control over their IS Knowledge**

7.8.1. All Company employees should be familiarised (against written acknowledgement) with their ISMS duties and documents within their job duties.

7.8.2. During employee recruitment they should be briefed on compliance with IS requirements against written acknowledgement.

7.8.3. Company employees should regularly undergo IS training (increase levels of IS knowledge).

7.8.4. Company employees responsible for setting and controlling IS requirements should continuously keep up their competency levels.

7.8.5. Company employees’ IS knowledge should be regularly tested.

7.9. **Organisation of Work with Third Parties**

7.9.1. In the process of Company activity it interacts with the following third parties:

– counterparties;

– government authorities;

- trading members;
- information agencies.

7.9.2. The conclusion of contracts with third parties should consider IS requirements approved both in the Company and in the organisation of the other party. Agreed information security requirements related to procedures for the exchange, processing, storage and dissemination of information, to the provision of external organisations with access to Company information assets should be formalised in the contract and/or agreement on confidentiality and non-disclosure of information by the parties.

7.9.3. The contract with counterparties on providing services of physical security and information infrastructure maintenance should consider the requirements for the procedure for access to the territory, premises and information assets of the Company.

7.9.4. Interaction with government authorities shall be regulated by appropriate federal laws and other normative and legal acts of the Russian Federation.

7.10. **Physical Security and Equipment Protection**

7.10.1. The Company should define and document requirements for the procedure for ensuring physical and equipment security, namely for:

- physical perimeter of security and tools for entry and exit control;
- protection from environmental threats (fires, flooding, civil disobedience acts and other forms of natural disasters and man-made catastrophes);
- work on limited access premises;
- equipment hosting and protection;
- use of supporting systems and wiring system;
- equipment maintenance and relocation;
- safe scrapping and equipment reuse;
- equipment use outside the Company’s territory.

7.10.2. Company information assets should be located on limited access premises within the established security perimeter with appropriate protection barriers and entry control mechanisms.

7.10.3. Arrangements for the access of Company employees and third party representatives to the territory and the premises should be documented.

7.11. **Technical and Organisational Measures to Ensure Information Security**

7.11.1. The Company should define and document requirements to the following groups of information security mechanisms:

- management of rights of access to Company information assets;
- acceptable usage of Company information assets;
- setting information infrastructure elements with respect to IS;
- use of information protection resources;
- management of portable equipment and removable media;
- backup;
- use of remote access.

7.11.2. The Company should control the issue of mobile equipment and removable media, as well as destruction of confidential information stored on them when they are no longer in use.

7.12. **Management of Company Information Infrastructure**

7.12.1. With respect to IT infrastructure management, the Company should set and document requirements for the following groups of security mechanisms:

- planning, acquisition and acceptance of IT infrastructure components;
- maintenance of and support for IT infrastructure components;
- management of IT infrastructure change and configuration.

7.12.2. The IS and BC Committee should control implementation of new tools for of information processing and protection.

7.13. **Management of Information Security Incidents**

7.13.1. The Company should collect and analyse information about IS system events and its vulnerable spots.

7.13.2. The Company should establish formal procedures for alerting and responding to IS incidents.

7.13.3. The results of analysing incident statistics should be used to detect recurrent or especially critical incidents and make decisions to develop preventive and corrective actions.

7.14. **Business Continuity Management**

7.14.1. The Company should implement the process of business continuity management to reduce to an acceptable level the loss caused by accidents and failures of Company IS by combining preventive and corrective measures.

7.14.2. The Company should develop and execute plans to restore main business processes and ensure the required level of information accessibility within the set dates following the interruption or failure. Plans for disaster recovery should be regularly tested and reviewed.

7.15. **Compliance with Legislative Requirements**

7.15.1. The Company should be guided by federal legislative requirements and other regulations of government authorities, requirements of Company internal documents and recommendations of international standards when ensuring IS and using materials protected by intellectual property rights. Attachment B contains the list of RF legislative acts and IS standards which the Company is guided by in building the ISMS.

7.16. **Policy on Using Licensed Software**

7.16.1. The Company should only use licensed software.

7.16.2. The Company should control installation of licensed software and register the licenses.

7.16.3. Safe storage of reference distributions and license keys should be organised.

7.17. **Internal Audits of Information Security**

7.17.1. The Company should regularly conduct internal ISMS audits to check that ISMS processes, procedures and control mechanisms:

– comply with IS requirements documented in the Company’s organisational and administrative documents;

– meet the ISO/IEC 27001 requirements, as well as applicable legislative requirements;

– are executed and supported in accordance with the established goals and objectives of information security;

– are efficient and effective.

7.17.2. The Company should determine and document audit criteria, the scope, frequency, methods, responsibility requirements for planning and conducting audits, as well as submitting reports on the results and on making records.

7.17.3. Selection of auditors and conducted audits should guarantee that the audit process is objective and unbiased. Auditors should not check their own work.

7.17.4. Deficiencies identified during internal audits should be removed by corrective actions. If an audit takes a decision to improve the ISMS in order to prevent potential deficiencies, such actions should be undertaken in the course of preventive actions.

7.17.5. Access to audit tools which help to check the performance of the Company's security systems should be protected to prevent potential misuse use and compromise. Access to audit results by Company employees and/or third party employees should be limited.

8. Compliance Control

8.1. The DORIS&BC shall be entrusted with control over compliance with the requirements of this Policy.

8.2. Employees of the Internal Control Service may additionally control the execution of this Policy’s requirements by conducting regular checks of the activity of Company units and individual employees for compliance of their actions with RF legislative requirements and internal documents regulating the Company’s IS activity.

9. Responsibility

9.1. All structural units of the Company shall be responsible for Company information security within their remit and in accordance with provisions set by this Policy and documents developed on its basis.

9.2. Heads of structural units shall be responsible for:

- timely communication of requirements of the Company's internal normative IS documents to employees of their units within their remit;
- allocation of Company information assets subject to protection and owned by their units, as well as agreement of requests for access to asset data;
- compliance by employees of their units with the requirements of the Company's internal normative IS documents.

9.3. All Company employees shall be personally responsible for their actions while working in the Company's information infrastructure and dealing with the protected information assets of the Company, as well as for meeting information security requirements established by this Policy and normative documents developed on its basis.

9.4. The IS Manager shall be responsible for controlling the execution and update of this Policy, as well as amendments thereto.

9.5. The Company's internal normative documents and RF legislation envisage responsibility for violating the requirements of this Policy and documents developed on its basis.

9.6. The Company's Senior Management shall resolve to apply and select liability upon the results of a security investigation depending on the feasibility of applying the measures in question, as well as on data about the intentional nature of the breach.

10. Review and Amendment Procedure

10.1. This Policy shall be regularly reviewed at least once every three years.

10.2. This Policy should be reviewed off-schedule in case of:

- amendments to RF statutory regulations, Company internal documents which set information security requirements;

- identified reduction in the overall level of Company information security (upon the results of an internal or external audit);

- material change to the Company's organisational and/or technology infrastructures, resources and business processes;

- identified material deficiencies in undertaking measures regulated by this Policy, as well as contradictions of its provisions with the other internal documents of the Company.

10.3. This Policy shall be reviewed and amended in accordance with the procedure established by the Company.

ATTACHMENT A: FORM OF DOCUMENTING DEROGATIONS OF IS INTERNAL DOCUMENTS

____

dated ____________ 20__

#	**Description of non-conformity**	**Non-conformity to which documents**	**IS Risks Related to Non-Conformity**	**Compensatory control procedures**	**Remedial plans**	**Action Owners**	**Review date** (3 years at most**)**

Findings:

____
____

____
____

Director, DORIS&BC

_________________ (_______________)

(signature) *(Full name)*

________________________ 20__

ATTACHMENT B. LIST OF STATUTORY DOCUMENTS REGULATING IS ACTIVITIES

Legislative acts regulating information security matters:

- The Criminal Code of the Russian Federation (Articles 137, 138, 140, 183, 272, 273, 274).
- Federal Law #149-FZ “On Information, Information Technologies and Information Protection” dated 27 July 2006.
- Decree # 188 of the President of the Russian Federation “On Approval of Confidential Data List” dated 6 March 1997.
- Decree # 1203 of the President of the Russian Federation “On Approval of the List of Data Constituting State Secret” dated 30 November 1995.
- Federal Law # 224-FZ “On Countering Illegal Use of Insider Information and Market Manipulation and Amendments to Some Legislative Acts of the Russian Federation” dated 27 July 2010.
- Federal Law # 63-FZ “On Electronic Signature” dated 06 April 2011.
- Federal Law # 325-FZ “On Organised Trading” dated 21 November 2011.
- Decree # 334 of the President of the Russian Federation “On Measures to Comply with Legislation to Develop, Produce, Sell, Operate Encryption Tools and Provide Services of Information Encryption” dated 03 April 1995.
- Decree # 351 of the President of the Russian Federation “On Measures to Ensure Information Security of the Russian Federation in Using Information and Telecommunications Networks of International Information Exchange” dated 17 March 2008.
- Regulations # 424 of the Government of the Russian Federation “On Special Aspects of Connection of Federal State Information Systems to Information and Telecommunications Networks” dated 18 May 2009.

Regulations and Procedural Documents Establishing Commercial Secret Regime:

- Federal Law #98-FZ “On Commercial Secret” dated 29 July 2004.
- The Civil Code of the Russian Federation (Articles 152.1, 857, 1465).

– Regulations #35 of the Government of the Russian Soviet Federative Socialist Republic “On the List of Data Which Cannot Constitute Commercial Secret” dated 5 December 1991 (as amended by the Regulations #731 of the Government of the Russian Federation dated 3 October 2002).

Regulations and Procedural Documents Ensuring Information Security of Personal Data:

– Federal Law # 152-FZ “On Personal Data” dated 27 July 2006.

– Labour Code of the Russian Federation # 197-FZ dated 30 December 2001. (Chapter 14 “Protection of Employee Personal Data”).

– Regulations # 1119 of the Government of the Russian Federation «On Approval of Requirements for Personal Data Protection in their Processing in Personal Data Information Systems” dated 1 November 2012.

– Regulations # 687 of the Government of the Russian Federation “On Approval of Special Aspects of Personal Data Processing without Using Automated Equipment” dated 15 September 2008.

– Regulations # 512 of the Government of the Russian Federation “On Approval of Requirements for Material Media of Biometrics Personal Data and Techniques for Storing Such Data outside Personal Data Information Systems” dated 06 July 2008.

– Basic Model of Personal Data Security Threats in their Processing in Personal Data Information Systems (approved FSTEC of Russia dated 15 February 2008).

– Methodology for Identifying Vital Threats to Personal Data Security in their Processing in Personal Data Information Systems (approved FSTEC of Russia dated 14 February 2008).

– Order # 21 of FSTEC of Russia “On Approval of Composition and Content of Organisational and Technical Measures to Ensure Personal Data Security in their Processing in Personal Data Information Systems” dated 18 February 2013.

– Recommended Practices for Ensuring of Personal Data Security by Encryption Tools in their Processing in Personal Data Information Systems Using Automated Equipment (approved by the FSB of the Russian Federation on 21 February 2008).

– Standard Requirements for Organising and Ensuring Operations of Encryption Tools Designed to Protect Information which does not Contain Data Constituting State Secret in case of their Use for Personal Data Security in their Processing in Personal Data Information Systems (approved by the FSB of the Russian Federation on 21 February 2008).

– Order # 274 of the Federal Service for Supervision of Communications, Information Technology, and Mass Media “On Approval of the List of Foreign States, which are not Parties to the Convention of the Council of Europe on Protection of Individuals in Automated Processing of Personal Data and Ensuring Appropriate Protection of Personal Data Owners” dated 15 March 2013.

– Model Regulations on Measures to Control (Supervise) within the Remit Execution of Requirements for Personal Data Security Established by the Government of the Russian Federation in their Processing of Personal Data Information Systems (approved by Order # 149/7/2/6-1173 of the FSB of the Russian Federation dated 08 August 2009).

Directive Documents of the FSTEC and FSB of the Russian Federation on Information Protection from Unauthorised Access:

– Order # 416/489 of the FSB of Russia, FSTEC of Russia “On Approval of Requirements for Protection of Information Contained in Public Information Systems” dated 31 August 2010.

– Order # 152 of the FAGCI “On Approval of Instruction on Organising and Ensuring Security of Storage, Processing and Transfer of Limited Access Information not Constituting State Secret via Communications Channels Using Crypto protection” dated 13 June 2001.

– Order # 638 of the FSTEC of Russia “On Approval of Requirements for Intrusion Monitoring Systems” dated 6 December 2011.

– Order # 28 of the FSTEC of Russia “On Approval of Requirements for Antivirus Protection Tools” dated 20 March 2012.

International Standards on Management of Information Security, Incidents and Business Continuity:

– International Standard ISO/IEC 27000:2012 (Information Technology — Security Techniques — Information Security Management Systems — Overview and vocabulary).

– International Standard ISO/IEC 27001:2013 (Information Technology — Security Techniques — Information Security Management Systems — Requirements).

– International Standard ISO/IEC 27002:2013 (Information Technology — Security Techniques — Code of Practice for Information Security Controls).

– International Standard ISO/IEC 27003:2010 (Information Technology — Security Techniques — Information Security Management System Implementation Guidance).

– International Standard ISO/IEC 27004:2009 (Information Technology — Security Techniques — Information Security Management — Measurement).

– International Standard ISO/IEC 27005:2011 (Information Technology — Security Techniques — Information Security Risk Management).

– International Standard ISO/IEC 27006:2011 (Information Technology — Security Techniques — Requirements for Bodies Providing Audit and Certification of Information Security Management Systems).

– International Standard ISO/IEC 27007:2011 (Information Technology — Security Techniques — Guidelines for Information Security Management Systems Auditing).

– International Standard ISO/IEC TR 27008:2011 (Information Technology — Security Techniques — Guidelines for Auditors on Information Security Controls).

– International Standard ISO/IEC 27010:2012 (Information Technology — Security Techniques — Information Security Management for Inter-Sector and Inter-Organisational Communications).

– International Standard ISO/IEC 27014:2013 (Information Technology — Security Techniques — Governance of Information Security).

– International Standard ISO/IEC 27015:2012 (Information Technology — Security Techniques — Information Security Management Guidelines for Financial Services).

– International Standard ISO/IEC 27035:2011 (Information Technology — Security Techniques — Information Security Incident Management).

– International Standard ISO 22300:2012 (Societal Security — Terminology).

– International Standard ISO 22301:2012 (Societal Security — Business Continuity Management Systems — Requirements).

– International Standard ISO 22313:2012 (Societal security — Business Continuity Management Systems — Guidance).

- International Standard ISO/IEC 27031:2011 (Information Technology — Security Techniques — Guidelines for Information and Communication Technology Readiness for Business Continuity).

- International Standard BS ISO/IEC 24762:2008 (Information Technology — Security Techniques — Guidelines for Information and Communications Technology Disaster Recovery Services).