APPROVED
by order of MC Delo
dated February 17, 2022 No.11

# INFORMATION SECURITY MANAGEMENT POLICY OF MC DELO (revision No. 1)

City of Moscow
2022

This Policy is a fundamental document regulating the activities of Limited Liability Company "Management Company "Delo" (hereinafter referred to as "MC Delo") in the field of information security.

The information security policy has been developed in accordance with the legal requirements of the Russian Federation and the provisions of international standard ISO/IEC 27001:2013.

The following **terms and concepts** are used in the Policy:

**Delo Group of Companies** (Group of Companies, Group, Delo Group), which includes MC Delo and companies directly or indirectly controlled by MC Delo.

**Management** - employees who report directly to the general director, or business unit managers.

**ISMS** - information security management system being a part of general risk based management system designed to create, implement, operate, monitor, analyze, maintain and improve information security.

**Business process** - a sequence of technologically related operations for provision of products, services and/ or implementation of specific activities of MC Delo.

**Asset owner** - an individual or entity administratively responsibility for managing manufacture, development, storage, use and safety of asset. The term "owner" does not mean that such person has actually ownership of the asset.

**Owner of information resources, information systems, technologies and their support -** an entity that owns and uses these objects and exercises powers of disposal within the limits established by the law.

**Accessibility of information** - a condition characterized by the ability of information system to provide unhindered access to information of entities authorized to do so.

**Information protection** - an activity aimed at preventing leakage of protected information, unauthorized and unintended impacts on protected information and means of access thereto.

**Information** – information about persons, objects, facts, events, phenomena and processes, regardless of the form of their presentation.

**Information security (IS)** – a state of protection of the interests of MC Delo.

**Information system** - a set of information contained in databases and information technologies and technical means that ensure processing thereof.

**Incident** - an unforeseen or undesirable security event (group of events) that has led (may lead) to functional failure of information system or threats to security of information (breach of confidentiality, integrity, availability).

**Information security incident** - one or a series of undesirable or unexpected information security events that have a significant probability of disrupting business processes or pose a threat to information security.

**Commercial secret** - confidentiality of information that allows its owner, under existing or potential circumstances, to raise revenue, avoid unreasonable expenses, hold a position on the market of goods, work, services or obtain any other commercial benefits.

**Confidential information** - restricted information that does not contain information constituting a state secret, access to which is restricted in accordance with the legislation of the Russian Federation.

**Confidentiality of information** - a state of information security characterized by ability of information system to ensure that information is kept secret from subjects not authorized to familiarize themselves with the same.

**Unauthorized access** - access to information or actions with information in violation of access control rules using standard means provided by computer technology or automated systems.

**Policy** - general objectives and guidelines formally expressed by the management.

**Privileges** - the rights of a trusted entity to perform any actions in relation to the objects of the system.

**Risk** - a combination of probability of event and consequences thereof.

**Threat** - a danger involving potential loss (damage).

**Information integrity** - resistance of information to unauthorized access or accidental exposure during processing by technical means, which may result in destruction and distortion of information.

## 1. General provisions

1.1. Information security refers to the state of information security, characterized by the ability of personnel, technical means and information technologies to maintain confidentiality, integrity and availability of information in the course of processing of the same using technical means.

1.2. The information security policy is approved by the Director General of MC Delo.

## 2. Purposes and objectives

2.1. The following strategic objectives are set in the field of information security management of MC Delo:

2.1.1. Protection of competitive advantages of MC Delo from threats in the field of information security.

2.1.2 Compliance with legal requirements, industry standards and contractual obligations in terms of information security.

2.1.2. Effective information security management and continuous improvement of the information security management system.

2.1.3. Adequate measures for protection against information security threats.

2.1.4. Maintenance of security of the assets of the Delo Group of Companies, including personnel, material and technical values, information resources, business processes.

2.2. Information security management system of MC Delo is designed to solve the following tasks:

2.2.1. Involvement of the management of MC Delo in the process of ensuring information security: information security activities are initiated and controlled by the management of MC Delo.

2.2.2. Compliance with the legal requirements of the Russian Federation: MC Delo implements information security measures in strict adherence to existing legislation, industry standards and contractual obligations.

2.2.3. Consistency of actions to ensure information, physical and economic security: activities aimed at ensuring information, physical and economic security are carried out on the basis of seamless interaction of concerned departments of MC Delo and are coordinated among themselves according to goals, objectives, principles, methods and means.

2.2.4. Application of economically feasible measures: MC Delo seeks to choose measures to ensure information security in view of the costs of their implementation, probability of information security threats and amount of potential losses as a result of their implementation.

2.2.5. Recording information security requirements: all information security requirements are recorded in internal regulatory documents developed in MC Delo.

2.2.6. Raising awareness about information security issues: recorded information security requirements are brought to the attention of employees of all business units of MC Delo and contractors as far as they are concerned.

2.2.7. Responding to information security incidents: MC Delo is engaged in systematic activities designed to identify, record and promptly respond to actual, ongoing and potential information security breaches.

2.2.8. Risk assessment: MC Delo implements measures on an ongoing basis to assess and manage information security risks, increase the level of security of information assets.

2.2.9. Taking into account the requirements of information security in project activities: MC Delo takes into account the requirements of information security in project activities. Development and recording of information security requirements is carried out at the initial stages of implementation of projects related to processing, storage and transmission of information.

2.2.10. Continuous improvement of the information security management system: improvement of information security management system is a continuous process.

## 3. Principles of information security

3.1. Consistency - the Delo Group of Companies considers assets as interrelated and mutually influencing components of a single system. The security system is built in view of the known channels for obtaining unauthorized access to information and the possibility of fundamentally new ways of implementing security threats.

3.2. Collective protection - responding to information security threats and incidents is carried out collectively by all cybersecurity units of companies controlled by MC Delo.

MC Delo acts as coordinator and competence center.

3.3. Completeness (complexity) - a wide range of measures, methods and means of information protection are used to ensure information security. Their integrated use involves coordination of mixed means in construction of integral protection system that covers all existing threat channels and does not contain any weaknesses at the junctions of its individual components.

3.4. Separation - the information security system is designed in such a way that the most protected security zone is located inside other protected zones.

3.5. Continuity - ensuring information security in MC Delo is a continuous dedicated process involving adoption of appropriate measures at all stages of asset lifecycle.

3.6. Reasonable sufficiency - means of asset protection that are adequate to actual threats (i.e. ensuring an acceptable level of potential damage in the event of threats) are selected on the basis of risk analysis.

3.7. Legality - when selecting and implementing measures and means to ensure information security, MC Delo strictly adheres to the legislation of the

Russian Federation, the requirements of regulatory legal and technical documents in the field of ensuring information security of MC Delo.

3.8. Controllability - all processes of ensuring and managing information security in MC Delo should be controllable, i.e. it should be possible to monitor and measure processes and components, promptly identify information security breaches and take appropriate measures.

3.9. Personal responsibility - responsibility for ensuring security of assets is imposed on each employee within his authorities.

## 4. Scope of application

Information security requirements apply to all regions of activity and to all companies controlled by MC Delo, to all information and information processing resources.

Compliance with this Policy is mandatory for all employees of MC Delo.

## 5. Persons involved in implementation of the Policy

5.1. General Director of MC Delo:

5.1.1. Approves the Policy, amendments and additions thereto.

5.1.2. Is responsible for implementation of the Policy in MC Delo;

5.1.3. Monitors the results of the Policy application and implementation of appropriate procedures in the Delo Group;

5.1.4. Monitors appropriate inspections.

5.1.5. Ensures control over implementation of measures taken by the executive bodies of companies controlled by MC Delo within the framework of information security management system.

5.2. Sole executive bodies of companies controlled by MC Delo:

5.2.1. Are responsible for compliance with the requirements of applicable legislation and local regulations of concerned company of the Delo Group of Companies.

5.2.2. Are responsible for implementation of the Policy in concerned company of the Delo Group of companies;

5.3. Responsible person:

5.3.1. Initiates updating of relevant local regulations.

5.3.2. Analyzes and evaluates adequacy and effectiveness of the system of measures taken, submits relevant proposals for improvement to the sole executive

body, prepares relevant reporting materials for the management and shareholders (members) of the Delo Group of companies.

5.3.3. Draws up a program, develops and implements appropriate procedures, ensures control over their implementation, organizes training events, individual counseling of employee, briefing in information security issues together with business units responsible for personnel management and legal support of activities.

5.3.4. Identifies and evaluates relevant risks.

5.4. Managers of business units of MC Delo and affiliated companies of MC Delo:

5.4.1. Ensure efficient operation of the information security management system.

5.4.2. Identify vulnerable information security processes and procedures.

5.4.3. Facilitate preliminary inspection or internal investigation.

5.4.4. Promptly inform the responsible person about any signs of information security incident.

5.4.5. Initiate application of disciplinary measures.

5.5. Employees of MC Delo and affiliated companies of MC Delo:

5.5.1. Comply with all requirements of the policy and local regulations of MC Delo in the field of information security.

5.5.2. Facilitate checks, preliminary inspections and internal investigations, inter alia, supply explanations and necessary documents.

5.5.3. Promptly report on any information security incidents.

## 6. Standards, activities and measures for protection of information

6.1. Information security management system

The information security management system (hereinafter - ISMS) is implemented in MC Delo in order to accomplish the stated purposes and objectives. ISMS is recorded in this policy, in the rules, procedures and job-related instructions. Recorded ISMS requirements are communicated to employees. Information security management tools are implemented based on the results of information security risk assessment.

6.2. Recording standard

In order to create integrated structure of regulatory documents of MC Delo in the field of information security, the regulatory documents being developed and updated shall comply with the following hierarchy:

6.2.1. This Policy is a first-level internal regulatory document on information security.

6.2.2. Second-level documents include instructions, procedures, regulations and other documents describing actions of employees of MC Delo in implementation of first- and second-level documents.

6.2.3. Third-level documents are reporting documents in support of fulfillment of upper level documents requirements.

6.3. Categorization of resources

All resources of MC Delo shall be identified and evaluated in the order of their importance. All valuable resources shall be compiled in a register (list). Information about resources of MC Delo facilitates protection of information that is proportional to the value and importance of resources. The following types of resources are present in the information systems of MC Delo: information resources containing confidential information and/ or restricted access information, including information about financial activities of MC Delo; publicly available information required for operations of MC Delo regardless of form and type of presentation thereof; information infrastructure, including information processing and analysis systems, technical equipment and software for information processing, transmission and displaying, including information exchange and telecommunications channels, information protection systems and facilities, sites and premises for accommodation of such systems.

Owner shall be assigned in respect of each resource, which shall be responsible for appropriate classification of information and resources related to information processing equipment, as well as for assigning and periodical checking access rights and categories defined by access control policies.

6.4. Classification of information

All information resources subject to protection shall be classified in the order of importance and access level. Classification of information shall be recorded and approved by the management of MC Delo. With a view to determine a category of resource, a resource owner, who stores or processes information, shall carry out classification of information. Classification shall be reviewed from time to time to maintain its relevance to resource category. Resources containing confidential or critical information shall be marked (labeled) accordingly.

6.5. Risk assessment and handling

Security requirements shall be defined in MC Delo though methodical risk assessment. Risk assessments shall identify, quantify and prioritize risks in accordance with risk acceptance criteria and business objectives of institution. The results of assessment shall determine the appropriate management response, priorities of information security risk management and a set of control mechanisms to protect against these risks. Risk assessment involves a systematic combination of risk

analysis and risk assessment. Besides, risk assessment and selection of control mechanisms shall be carried out from time to time in order to:

consider changes in business requirements and priorities;

take account of new threats and vulnerabilities;

make sure that the implemented facilities continue to be efficient.

Before processing each risk MC Delo shall select criteria to determine acceptability of this risk. Risk can be accepted if its magnitude is sufficiently small and the cost of processing is unreasonable for MC Delo. Such decisions shall be recorded. One of the following decisions on processing shall be made in respect of each assessed risk:

use of appropriate control mechanisms to reduce risk to acceptable level;

conscious and objective acceptance of risk, if it definitely complies with the Policy of MC Delo and meets risk acceptance criteria;

avoiding risk through preventing any actions that could serve as triggering events;

transfer of risks to any other party (outsourcing, insurance, etc.).

6.6. Information security training

All employees shall receive periodic training in information security policies and procedures adopted in MC Delo. Timing and frequency of information security training are determined at the initiative of the Deputy Director for Cybersecurity of Information Technology and approved by the authorized management body of MC Delo.

6.7. Access control

Employees of business units are the main users of information in the information system of MC Delo. Authorization level of each user is determined on an individual basis. Each employee shall exercise solely the rights vested in him/ her in relation to information to be handled by such employees in accordance with his/ her job duties. Access of users to handle information resources is strictly regulated. Any changes in composition and authorities of subsystem users shall be made in accordance with the established procedure. Registered accounts are divided as follows:

Subscriber accounts – designed to authenticate users of MC Delo;

System accounts – used for the needs of operating system;

Service accounts – designed for functioning of individual processes or applications.

6.8. Privilege management

Access of employee to information resources of MC Delo shall be authorized by owners of relevant information resources. Access control is maintained in accordance with the established procedures. Granting and using privileges shall be

strictly limited and controlled. Distribution of privileges shall be managed through the process of registration of these privileges.

6.9. Password management

Password is tool of verification of user's identity for gaining access to information system, information resource or service providing for identification and authentication based on information known to user only.

Password management shall ensure the following:

setting requirements for password complexity - it is necessary to set requirements for password length, character set and number of input attempts;

ensuring secrecy of personal passwords;

passwords assigned by software manufacturer shall be changed immediately after installation;

ensuring compliance with the requirement to periodical change of user password;

use of other technologies for user identification and authentication, in particular, biometric technologies, electronic signature verification and hardware (smart cards, e-Token/ ruToken, chips, etc.), if technically feasible.

6.10. Work on the Internet

Access to the Internet is provided to employees of MC Delo for the purpose of performance of their job duties that require direct connection to external information resources to the extent minimally sufficient for these purposes.

When using the Internet, it is prohibited to:

use Internet access provided by MC Delo for personal purposes;

use unauthorized hardware and software tools that allow unauthorized access to the Internet;

commit any actions aimed at disrupting normal functioning of elements of information technologies of MC Delo.

MC Delo reserves the right to block or restrict users' access to Internet resources, which content is not related to performance of job duties, as well as to resources, which content and orientation are prohibited by the law.

Information about Internet resources visited by the employees of MC Delo is recorded for subsequent analysis and, if necessary, can be submitted to Business unit managers, as well as to the Management of MC Delo for control.

6.11. Protection against malicious software

Systematic and automated operations shall be implemented in MC Delo with a view to prevent penetration of malicious software and any negative effects of the same.

6.12. Electronic digital signatures

Electronic digital signatures provide protection of authentication and integrity of electronic documents and can be used for any form of document processed electronically.

Electronic digital signature is an analogue of handwritten signature.

It is necessary to take particular care in order to maintain confidentiality of private key of electronic digital signature, which should be kept secret, since anyone with access thereto can sign documents (payments, contracts), thereby forging a signature of key owner.

Transfer of personal electronic digital signature to any third parties (deputies, acting secretaries, assistants and any other administrants) is strictly prohibited.

6.13. Information security incident management

A formal procedure for reporting information security incidents in MC Delo, as well as a procedure for responding to such incidents, including actions to be performed upon receipt of reports of any incident, are developed at the initiative of the Deputy Director for Cybersecurity of Information Technology and approved by the authorized management body of MC Delo. Mechanisms and automated monitoring to assess and track the types of incidents, their scale and associated costs are developed at the initiative of the Deputy Director for Cybersecurity of Information Technology and approved by the authorized management body of MC Delo.

The procedure for reporting information security incidents on a mandatory basis provides for measures to promptly inform data subjects exposed as a result of any incident.

6.14. Continuity and recovery management

Plans allowing to continue or restore operations and to ensure the required level of information availability in a timely manner after interruption or failure of critical business processes are developed at the initiative of the Deputy Director for Cybersecurity of Information Technology and approved by the authorized management body of MC Delo. Each business continuity support plan contains information on conditions precedent to its execution and employees responsible for implementation of each section of plan. Contingency plans are amended as far as new requirements appear. A specific owner is assigned for each plan. The rules of actions in contingency situations, manual disaster recovery plans and business resumption plans are the responsibility of owners of relevant resources or related processes.

6.15. Information security audit

MC Delo conducts internal checks of ISMS at scheduled intervals. The main objectives of such checks are as follows:

assessment of current security level of information systems;

identification and localization of vulnerabilities in the system of information system protection;

analysis of risks associated with potential implementation of security threats in respect of information resources;

assessment of compliance of information systems with the requirements of internal regulatory documents of MC Delo;

drawing up recommendations for ISMS improvement by introducing new information security measures and enhancing efficiency of the existing ones.

The tasks to be solved during ISMS checks and audits include the following:

collection and analysis of benchmark data on organizational and functional structure of information systems required for assessment of information security status;

analysis of the existing security policy and other organizational and administrative documents on information protection for their completeness and effectiveness, as well as drawing up recommendations for their development (or revision);

feasibility study of security mechanisms;

verification of selection and configuration of information security tools, formulating proposals for the use of existing and installation of additional security tools to increase information system reliability and security level;

analysis of information security incidents and minimization of potential damage as a result of the same.

In the course of ISMS audits the management and employees of MC Delo are obliged to lend assistance and provide all information required for audit.

6.16. Transfer of information to third parties

When MC Delo transfers to any third party any information, in respect of which such third party acts as the owner or operator, it is necessary:

to prevent transfer of information without properly executed contractual obligations between the owner of information and MC Delo directly providing for consent of the owner of information to transfer to any third parties;

in case of transfer of information, in respect of which MC Delo acts as a copyright holder or owner, or if information is transferred with the consent of third parties, MC Delo undertakes to include the requirements to comply with the provisions of this policy in contractual obligations.

## 7. Liability

In case of violation of the established rules for handling information assets by any employee, the access rights to such assets of employee, regardless of his position,

may be restricted, and such employee may be held liable in accordance with the legislation of the Russian Federation.

## 8. Final provisions

8.1. This Policy shall amended and cancelled by order of the General Director.

8.2. This Policy is subject to revision if changes are made to:

the existing legislation of the Russian Federation;

internal regulatory documents of the Company.

8.3. This Policy shall be updated by the Deputy Director for Cybersecurity of Information Technology.

8.4. In case of revision and amendments to this Policy, all concerned parties and entities shall be informed thereof by publishing the policy on the public resource of MC Delo.

8.5. The Deputy Director for Cybersecurity of Information Technology may provide explanations on the application of this Policy.

8.6. Control over implementation of the requirements of this Policy is imposed on the Deputy Director for Cybersecurity of Information Technology.

8.7. If a reference is made in the text of this Policy to any document that has been amended (invalidated) after the date of approval of this Policy, it is required to use the current version of this document. If a reference is made to any cancelled document, the relevant section of the Policy shall be applicable to the extent not affected by the reference to such void document.

_____