Public Joint Stock Company Uralkali

Π 13-2019

APPROVED:

By Order No. 2447 dated
19.12.2019 of the General Director
“On approval and implementation
of the Information Security Policy
of PJSC Uralkali”

INFORMATION SECURITY POLICY
of PJSC Uralkali

3rd edition

Berezniki, Perm Region

Preamble

1. This Policy WAS DEVELOPED by the Department for Methodology and Information Security Process Management of the Information Technology Directorate of PJSC Uralkali

2. This Policy WAS IMPLEMENTED in compliance with the Order No. 2447 dated 19.12.2019.

   Date of implementation 19.12.2019

3. This Policy WAS DEVELOPED as a replacement of the Information Security Policy of PJSC Uralkali approved in compliance with Order No. 444 dated 17/03/2016

Contents

1. Area of application

1.1 The Information Security Policy of PJSC Uralkali (hereinafter referred to as the 'Policy') is a framework document that reflects the strategy of the Company regarding the provision of information security (hereinafter 'IS'). The Policy was developed in order to establish the objectives, principles and approaches required to ensure a high standard of information security at Uralkali Group.

1.2 The Policy applies to all organisations within Uralkali Group: this includes all employees at Uralkali Group, as well as external organisations who must also familiarise themselves with and apply this Policy in their processes when working with Uralkali Group.

1.3 The Information Security Policy shall be implemented following approval by each director of the different Uralkali Group organisations (under a relevant order), or an organisation's own bespoke information security policy will be implemented that best reflects the specific nature of the business of the relevant organisation, provided that it does not contradict the requirements of this Policy.

1.4 The relevant internal documents that detail the Policy must not contradict it. In case of any contradictions, the relevant provisions will be brought in line with the Policy at the time when they are next due to be updated.

2. Regulatory framework

This Policy was developed using the following sources:

- Legislative and regulatory acts for information security in the Russian Federation;
- Guidelines and methodological documents of the Federal Service for Technology and Export Control (FSTEK) and the Federal Security Service (FSB) of Russia
- ISO/IEC 27000 international standards series
- PJSC Uralkali's Code of Corporate Culture

3. Terms and definitions

The following terms and definitions are used in this Policy:

Uralkali Group – PJSC Uralkali and its subsidiary companies. The composition of Uralkali Group may change in the case that new subsidiaries of PJSC Uralkali are formed.

Information security – the practice of information (data) protection – information security implies the confidentiality, accessibility and integrity of data is ensured

Information – this term encompasses any form of data (e.g. communications, information) regardless of the nature of its provision (e.g. print/electronic etc.).

4. Abbreviations

Group – Uralkali Group;
Company – Public Joint Stock Company Uralkali;
ISMS – Information Security Management System.

5. General provisions

5.1 Information is a critical Company asset, and information security measures are a key requirement for achieving the mission and vision of the Company. These measures are

part of the foundations which support the communication of the Company's corporate culture and preserve the values, established under the Code of Corporate Culture.

5.2 Information security is essential for achieving the Company's strategic goals and minimising the risks it encounters.

5.3 The Company uses a series of international standards (ISO/IEC 27000) as a methodological basis for the establishment and development of its system of information security.

5.4 In order to control and assess the level of maturity of information security processes, we have selected a range of metrics from the integrated CMMI (Capability Maturity Model Integration) model. In accordance with this model, the Company aims to maintain maturity level 4.

6. Key purpose and objectives

6.1 Ensuring information security in the Company has the following purpose:

1) Supporting the Company's strategic goals, listed below:
   - Ensuring the safety of production processes;
   - Maintaining existing production;
   - Meeting the security needs of the business;
   - Compliance with legal requirements;
   - Increasing the availability of equipment
   - Timeliness and quality in the provision of IT services and in supporting these services.

2) Preventing all types of negative consequences and pre-empting risks that may occur, in the case that internal and external information security threats materialise.

6.2 Ensuring information security in the Company has the following key purposes:

1) Creating a comprehensive, effective and manageable information security system that meets the requirements of the business, as well as the requirements of Russian and international laws, standards and global best practices;

2) Creating and continuously developing an information security management system (ISMS);

3) Creating a system of internal regulatory and administrative documents that detail the provisions of the Policy and regulate information security processes;

4) Forecasting, identifying and preventing threats and information security incidents;

5) Effectively managing information security risks;

6) Ensuring compliance with the Company's legal and administrative requirements;

7) Continually raising awareness of information security matters among the Group's employees.

7. Key principles

7.1 The Company implements information security processes in compliance with the following principles:

1) Legality. All information security measures in relation to information and information resources that must be protected in compliance with the law must be implemented in strict compliance with the indicated requirements;

2) Risk-orientation. The decision-making regarding ensuring information and information resource security (that are not subject to the requirements of the law) must be taken on the basis of a risk assessment and evaluation of the consequences of information

security threats materialising, in relation to the indicated objects of protection. Information security risks must be assessed within the framework of the risk management system of the Company;

3) Consistency and comprehensiveness. The required level of security must be achieved by creating a comprehensive system for information security that includes all the required legal, organisational and technical considerations of best practice information protection, aimed at blocking (neutralising) all current information security threats.

4) Compatibility and comparability. The measures of information protection must be commeasurable with legal requirements and the results of information security risk assessments;

5) Timeliness. Information protection measures must be preventative in nature;

6) Continuity. Ensuring information security is a continuous process applied at all stages of the lifecycle of protectable data – from creation to destruction;

7) Improvement. The system of information security must continuously develop to account for new threats, adjustments and developments in legal requirements and global best practices;

8) Minimisation of authority (in having to deal with information security processes). Access to information security must be limited and manageable, and in accordance with employees' job descriptions;

9) Control and assessment. The processes of ensuring and managing information security must be regularly controlled from both an external and internal perspective, in order to guarantee their compliance with applicable requirements and in passing performance assessments. The indicated results of these assessments must also be regularly analysed;

10) Personal liability. Employees are responsible for ensuring information security within the framework of their own job duties.

8. IS System

8.1 In order to achieve the Company's goals and to implement the principles set out above which look to ensure information security, the Company is creating an Information Security System.

8.2 The Information Security System is comprised of:

1) ISMS;
2) A detailed suite complex of technical processes for information protection;
3) Separate information security subsystems for each type of protected data form.

8.3 The internal and administrative documents that regulate information security processes at each level of the system are compiled in a single area for the Company's information security.

8.4 The composition and structure of the ISMS (including the composition of protectable data, the system of role and responsibility distribution, the documentation system, and the processes and measures for ensuring information security), as well as the composition of further subsystems of information security, shall be determined and regulated by other Company internal documents (standards, regulations, methodologies, instructions, etc.) that detail and clarify the provisions of this Policy.

9. Liability

9.1 Company Management is responsible for the implementation of this Policy.

9.2 The heads of directorates and subdivisions, as well as employees of the Company, are liable for performing their duties towards ensuring and complying with the requirements of IS in compliance with ISMS documents, and similarly the representatives of third parties who have access to the information resources of the Company are required to comply with the IS Policy within their contractual undertakings.

9.3 Different divisions of the Company (where applicable) are liable for the achievement of the goals and tasks set by the Company's management and for monitoring compliance with the requirements reflected in the internal documents of the ISMS. All exceptions from the indicated requirements shall be approved by the liable divisions of the Company.

10. Final provisions

10.1 This Policy is a subject to be revised in the result of significant changes in the Company's development, legal requirements of the Russian Federation or local laws in the areas of the Company's presence, or if there are major changes to other organisations within Uralkali Group.

10.2 The Policy and all amendments thereto shall be approved by the Uralkali CEO.