


**INFORMATION  
SECURITY POLICY OF  
KPI Inc. LLP**

**Atyrau  
2022**

	<b>Политика информационной безопасности</b>	
	Редакция 1	Дата введения: с момента утверждения

**Developed by:**  
**Leading Information Security**  
**Specialist of the Corporate**  
**Security Department**  
                     S. Solovyov  
**June 24, 2022**

**Checked by:**  
**Director of the Corporate**  
**Security Department**  
                                     N. Urazbayev  
**July 11, 2022**

**Approved by the**  
**resolution of the Board of**  
**KPI Inc. LLP.**  
  
**dated August 18, 2022**  
**№ 21/22**

### Content

Section No.	Section, chapters	Page
1.	Purpose of the document and general provisions	3
2.	Main goals and objectives of information security	3
3.	Basic principles in the field of information security	4
4.	Responsibility	4
5.	Final provisions	4

## **1. Purpose of the document and general provisions**

1.1 The achievement of the strategic goals of KPI Inc. LLP (hereinafter referred to as the Partnership) is closely related to the management of information, which is an important information resource. Information security (hereinafter referred to as information security) is one of the critical factors for the successful and stable operation of the Partnership.

1.2 The Information Security Policy (hereinafter referred to as the Policy) is a first-level document, the detailed requirements of the Policy are defined in other regulatory documents of the Partnership, as well as in accordance with regulatory legal acts of the authorized body.

1.3 The management of the Partnership declares its commitment to the Policy that has been announced, disseminated, implemented and maintained at all levels of the Partnership's management.

## **2. Main goals and objectives of information security**

2.1 The policy is aimed at achieving the following main objectives:

- 1) protecting information from real and potential threats;
- 2) minimization and localization of consequences when exposed to threats;
- 3) development of corporate culture in the field of information security.

2.2 Main objectives of the Policy are:

- 1) identification, prevention and neutralization of real and potential threats to information security, as well as the establishment of the causes and conditions of their occurrence;
- 2) improving the mechanisms of rapid response to information security threats;
- 3) effective information security risk management;
- 4) informing, training, and monitoring the knowledge of the Partnership's employees on information security issues.

2.3 In order to solve these tasks, the Partnership implements an Information Security Management System (hereinafter referred to as ISMS) based on international standards for information security and the requirements of the legislation of the Republic of Kazakhstan, confirming the ability to choose adequate and proportional information security management tools that ensure the security of information resources.

2.4 The ISMS, being part of the general management system of the Partnership, is documented in this Policy, as well as other ISMS documents detailing and developing the provisions set out in the Policy at the level of their practical implementation and are mandatory for all employees of the Partnership, as well as representatives of third parties who have access to the information resources of the Partnership.

## **3. Basic principles of activity in the field of information security**

3.1 Within the framework of the ISMS, the provision of information security in the Partnership is carried out in accordance with the following basic principles:

- 1) legality;
- 2) process approach;
- 3) comprehensive use of methods, methods and means of protection;
- 4) following best practices;
- 5) reasonable sufficiency;

6) personal responsibility.

#### **4. Responsibility**

4.1 The management of the Partnership monitors the implementation of the Policy.

4.2 The heads of functional units, structural divisions, employees of the Partnership are responsible for the performance of their duties to maintain the activities and ensure the requirements of the IS in accordance with the documents of the ISMS, and representatives of third parties who have access to the information resources of the Partnership in accordance with contractual obligations.

4.3 The structural unit for ensuring the information security of the Partnership is responsible for the goals and objectives set by the management of the Partnership, as well as monitoring compliance with the requirements reflected in the documents of the ISMS. All exceptions to these requirements must be agreed with the structural unit for the provision of information security.

#### **5. Final provisions**

5.1 The policy is reviewed in case of significant changes in business development, as well as requirements of the legislation of the Republic of Kazakhstan or regulatory authorities.

5.2 The Policy, as well as all changes to it, are approved by the Management Board of the Partnership.

5.3 The Policy is publicly available on the official website of the Partnership [www.kpi.kz](http://www.kpi.kz) .