INFORMATION SECURITY POLICY

Astana
2023

1.General provision

This Policy of information security of the information system of Qazaq Green Certificate Registry (hereinafter - Policy) defines the system of information security principles and is a systematic statement of the goals and objectives of protection, basic principles of construction, organizational, technological and procedural aspects of information security at the operator of Qazaq Green Certificate Registry - Association of RES "Qazaq Green" (hereinafter - Organization).

The Policy takes into account the current state and immediate prospects for the development of information technologies in the Organization, the goals, objectives and legal basis for their operation, modes of operation, and also contains a list of security threats to the objects and subjects of information relations of the Organization.

The requirements of this Policy apply to all structural subdivisions of the Organization.

The Policy is developed in accordance with the Laws of the Republic of Kazakhstan "On Electronic Document and Electronic Digital Signature", regulatory legal acts of the Republic of Kazakhstan, as well as other regulatory legal acts of the Republic of Kazakhstan.

Policy is a methodological framework for:

1) Formation and implementation of a unified information security policy in the Organization;

2) organization of work to identify information subject to protection, justify the level of its confidentiality and document it in the form of relevant lists;

3) making managerial decisions and developing practical measures to implement information security policy;

4) developing a set of coordinated measures aimed at identifying, reflecting and eliminating the consequences of the realization of various types of threats to information security;

5) coordination of activities of structural subdivisions of the Organization in carrying out works on creation, development and operation of information technologies in compliance with the requirements for information security;

6) developing proposals to improve legal, regulatory, technical and organizational information security in the Organization.

Protection of information resources is carried out within the framework of the Information Security Management System corresponding to:

- requirements of the information security standard ST RK ISO/IEC 27001-2015.

- requirements of the legislation of the Republic of Kazakhstan, regulatory and contractual obligations of the Organization in terms of information security;

- this Information Security Policy of the Organization.

The scope of the Organization's Information Security Management System is:

information security management with respect to the uninterrupted functioning of the Organization's information systems.

The Organization's management fully assumes responsibility for information security activities in the Organization, declares its commitment to the above objectives and principles, and obliges all personnel of the Organization to do the same. Employees of the Organization are personally responsible for compliance with the requirements of ISMS documents and are obliged to report all detected violations in the field of information security

This Information Security Management System Policy is subject to regular review, at least once a year.

The policy aims to achieve the main objectives:

1) Protecting the integrity of information used and processed in the Organization;
2) Preserving the confidentiality of critical information resources;
3) ensuring accessibility of processed information for registered users;
4) ensuring continuity of the main business processes functioning in the Organization.

In order to achieve the above goals, the following tasks need to be accomplished:

1) active participation of management in managing the information security of the enterprise;
2) raising staff awareness of the risks associated with information resources;
3) clear distribution of responsibilities and duties of information security staff;
4) differentiating access of registered users to hardware, software and information resources of the enterprise;
5) logging user actions in system logs when using network resources;
6) control of correctness of system users' actions by analyzing the contents of these logs;
7) protection against interference by unauthorized persons in the operation of information systems;
8) controlling the integrity of the software used, the program execution environment and its recovery in case of violation, as well as protecting systems from the introduction of malicious codes;
9) protection of information with limited dissemination, personal data from leakage through technical channels during its processing, storage and transmission via communication channels;
10) ensuring authentication of users of information systems and resources;
11) timely identification of information security threats, causes and conditions contributing to damage;

12) creating conditions for minimizing and localizing the damage caused by unlawful actions of individuals and legal entities;

13) maintaining the practice of disciplinary action in case of violation of the Information Security Policy;

14) to address the consequences of an information security breach;

15) development and implementation of rules and instructions on information security, control over fulfillment of the relevant requirements by the company's employees;

16) implementation of measures to assess and manage information risks;

17) improving the information security management system.

2. Management's responsibilities and liabilities

Effective security requires accountability, a comprehensive definition and recognition of security responsibilities. Management should be responsible for all aspects of security management, including risk management decision-making. Its individual factors, such as the type, form of incorporation, size and structure of the organization, will affect the level at which these responsibilities are defined. Information security is an interdisciplinary topic that applies to all users within the Enterprise. Properly defining and delineating accountabilities, specific job duties and responsibilities should ensure that all critical tasks are performed effectively and proficiently.

Management is directly involved in information security related issues in accordance with the organization's (business) objectives, laws and regulations.

The management supports the specified level of information security by implementing a management system, as well as by distributing the duties and responsibilities of personnel for its provision (order on appointment of responsible persons, job descriptions, etc.).

Guidance:

1. Formulate, review and approve information security policy and monitor the effectiveness of information security policy implementation;
2. Provide clear governance and meaningful support for information security initiatives;
3. Provide resources for information security;
4. Ensure coordination of information security controls in the organization;
5. Approve the roles and responsibilities of information security officers in the organization through job descriptions, orders, decrees, etc.;
6. Initiate ideas, plans and programs to maintain information security awareness, determine the need to train users and administrators in security methods and procedures, and define responsibilities related to software and hardware

installation and maintenance;

7. Determine the need for specialist consultation within the organization or from outside the organization on information security issues, review and coordinate the results of the consultation across the organization;

8. Clearly establish the responsibility of department heads for various safety assets and processes, details of this responsibility should be documented, levels of authority should be clearly defined and documented (material responsibility act);

9. Maintaining the practice of disciplinary action in case of violation of the Information Security Policy;

10. liquidation of consequences of information security breach.

Employees should be familiarized with the measures of responsibility for disclosure of information in accordance with their functional duties, as well as with the measures of responsibility for possible violations.

IS maintenance personnel in case of violation of the requirements of the IS policy clauses shall be held administratively or otherwise liable in accordance with the current legislation of the Republic of Kazakhstan. IS administrators shall be held responsible in accordance with their responsibilities in accordance with the Instruction on Assignment of Functions and Authorizations of the Server Administrator. In particular, IS resource administrators ensure the continuous functioning of the network and are responsible for the implementation of technical measures necessary for the implementation of the security policy.

3. Basic principles of information security

The basic principles of information security are:

1) compliance with the requirements of the legislation of the Republic of Kazakhstan;

2) compliance with international and national standards in the field of information security in force in the territory of the Republic of Kazakhstan;

3) continuous and comprehensive analysis of the information space in order to identify vulnerabilities of information assets;

4) identification of cause-and-effect relationships of possible problems and building on this basis an accurate forecast of their development;

5) adequate assessment of the degree of impact of the identified problems;

6) comprehensive use of methods and means of protection of computer systems, covering all significant channels of threat realization and not containing weaknesses at the junctions of its individual components. Protection should be ensured by physical means, organizational, technological and legal measures. At the same time, measures taken to ensure information security should not complicate the achievement of statutory objectives, as well as increase the labor intensity of technological processes of information processing;

7) effective implementation of the protective measures taken;

8) flexibility of the means of protection to ensure variation of the level of protection due to possible changes in external conditions and requirements over time;

9) improvement of measures and means of information protection on the basis of continuity of organizational and technical solutions, analysis of information systems functioning taking into account changes in methods and means of information interception and impact on their components, regulatory requirements for protection, experience of other organizations, both domestic and foreign, achieved in this field;

10) continuity of safe operation principles.

11) mandatory and timely detection, suppression of attempts to violate the established rules of information security. Control of users' activity, each means of protection and in relation to any object of protection shall be carried out on the basis of application of means of operational control and registration and shall cover both unauthorized and authorized actions of users;

(12) Clearly define functional and information security objectives in documents to avoid uncertainty in organizational structure, personnel roles, approved policies, and the inability to assess the adequacy of protective measures taken;

13) determination of personal responsibility for ensuring the security of information and its processing system for each employee within the limits of his/her authority. In accordance with this principle, the distribution of rights and responsibilities of employees should be structured in such a way that in case of any breach the circle of culprits is clearly known or minimized;

14) ensuring availability of services and facilities for its clients and counterparties within the established timeframes determined by relevant contracts (agreements) and/or other documents;

15) observability and assessability of information security provision, the result of application of protective measures should be clearly observable (transparent) and could be assessed by an authorized specialist;

16) classification of processed information, determination of its importance level in accordance with the legislation of the Republic of Kazakhstan.

4. Personnel policy on information security

Staff roles and responsibilities are clearly defined in job descriptions and communicated to candidates at the time of hire.

Employees sign the terms and conditions of their employment contract, which sets out their responsibilities and the company's responsibilities regarding information security.

Employees and third-party representatives using the organization's

information processing facilities must sign an agreement in accordance with information security requirements to mitigate risks from theft, fraud and misuse of equipment, as well as threats to information security.

A Confidentiality and Non-Disclosure Agreement shall be signed by the employee, contractor, or third party user prior to granting access to information processing facilities.

Verification of all candidates for permanent employment shall be carried out in accordance with the applicable labor legislation of the Republic of Kazakhstan with respect for the confidentiality of personal data. The following information provided by the candidate is subject to verification:

1) references from previous jobs;
2) applicant's resume;
3) documents on education and professional qualifications;
4) identity documents;
5) other information requiring clarification.

Information on all employees hired on a permanent basis should be collected and processed in accordance with the applicable labor laws of the Republic of Kazakhstan.

Employees shall be familiarized with the requirements of this Policy, information security rules and instructions, with mandatory signing of the familiarization sheet, in order to raise awareness, inform about the procedures of incident response and prevention.

It is necessary to control the return of all assets (computer equipment, official documents, electronic media, etc.) used by employees at the end of their employment contract, and, in case an employee uses personal equipment, to ensure that the information is transferred to the head of the relevant division (responsible specialist) or that the information is deleted from the equipment by non-recoverable methods.

Access rights to information systems and resources are revoked upon termination of an employee's employment contract (dismissal) or are subject to review upon changes in the employee's duties and functions.

Passwords for accounts that remain active must be changed at the time of termination of employment due to extended business travel, vacation, or termination of employment.

5. Revision of the Information Security Policy

Provisions of the Enterprise information security policy require regular review and adjustment at least once a year according to the plan.

An unscheduled review of the Security Policy shall be conducted in the event of:

1) making material changes to the IP;
2) changes in legislation, organizational structure;

3) the occurrence of information security incidents.

When making changes, consideration shall be given to:

1) the results of information security audits, as well as the results of previous audits;
2) recommendations of independent information security experts;
3) significant threats and vulnerabilities of the information system;
4) information security incident reports;
5) recommendations of public authorities.

Revision of the Policy is performed by the specialists responsible for its development, implementation and includes assessment of the possibility to improve its provisions and the information security management process in accordance with the changes.

The revision of the information security policy shall be performed in accordance with the guidelines for the implementation of ST RK ISO/IEC 27002-2009.

This Policy shall be subject to mandatory revision based on the results of analysis and assessment of information security risks for the IS and shall be updated as necessary.

The revised information security policy shall be approved by the authorized persons.

FAMILIARIZATION SHEET

№	Surname, first name, patronymic	Position	Personal signature	Date
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				