MAGTICOM

Information Security Policy

18.12.2023

Information security policy

1. Content

1.1. According to the Law of Georgia "On Information Security", three categories of critical information system entities are established. According to the law, the entity of the second category of critical information system is the organizations of the telecommunications sector. According to the Resolution N646 of the Government of Georgia dated December 31, 2021, "Magticom" LLC (ID number: 204876606, Address: Politkovskaya St. N7, 0186 Tbilisi, Georgia) is an entity of the second category of critical information system.

1.2. For the effective implementation of Magticom's goals, it is important to ensure the security of the organization's information assets and to protect them at an appropriate level (confidentiality, availability and integrity), which is achieved, among other means, by implementing an information security management system.

1.3. Magticom's information security management system consists of: policies, procedures, guidelines, related resources and activities that the organization manages collectively to protect its information assets.

1.4. Magticom's information security policy describes the main principles of information security management system operation in accordance with the Law of Georgia "On Information Security" and the ISO/IEC 27001 standard.

2. Definition of terms

For the purposes of this policy, the terms used therein shall have the following meanings:

2.1. **Information security** – activities that ensure access, integrity, authentication, confidentiality and continuous operation of information and information systems;

2.2. **Information asset** - all information and knowledge (in particular, technological means of information storage, processing and transmission, employees and their knowledge about information processing), which are valuable for the entity of a critical information system;

2.3. **Information security management system** – is part of the management system, which is a systematic approach to establishing, enforcing, managing, monitoring, reviewing, maintaining and improving an organization's information security. The information security management system is based on the organization's risk assessment and risk acceptance criteria, which are developed for the effective treatment and management of risks.

2.4. **Availability** - the characteristic of accessing and using the asset in accordance with the request of the authorized entity;

2.5. **Confidentiality** - a characteristic of an asset, according to which the asset is accessible only to authorized individuals, entities or processes;
2.6. **Integrity** - the characteristic of accuracy and completeness of an asset;
2.7. **Organization** - Magticom LLC;
2.8. **Risk analysis** - the process of assessing the source of risk and the level of risk, on the basis of which risk assessment is made and a decision on risk treatment is made. Risk analysis also includes primary risk analysis and assessment (measurement);
2.9. **Risk management** - implementation of coordinated actions necessary for management and control of the organization, taking risks into account;
2.10. **Risk treatment** - the process of changing the risk, which may include avoiding the risk by refusing to start or continue an activity, which in turn includes:
- May involve accepting or increasing risk in order to exploit opportunities, namely:
- removing the source of risk;
- change of address;
- changing the results;
- sharing the risk with another party;
- Keeping Rick aware and avoiding risk;

2.11. **Responsible Person** - The person responsible for an asset, risk or other relationship can be defined as a specific role and person, as well as a structural unit.

3. Purpose of information security policy

The purpose of the information security policy is to define the basic principles and approaches needed to ensure information security in the organization;

4. Scope of the policy

4.1. The information security policy applies to the organization:
4.1.1. To all employees (including trainees);
4.1.2. To all business processes (main and supporting processes);
4.1.3. To all types of information assets;
4.1.4. To third parties who have access to the organization's information assets or participate in their processing.
4.2. The scope is specified in the information security management system scope document.

5. Information Security Board

5.1. The organization creates an information security Board, the purpose of which is to ensure the effective functioning, compliance and adequacy of the information security management system.

5.2. The purpose, tasks and functions of the Information Security Board, the composition of the Board, the regulations of the Board and the details of the organizational and technical support are outlined in the Regulations of the Board (Information Security Board regulations).

6. Information security manager

6.1. The information security manager is accountable to the information security board;

6.2. The obligations and functions of the information security manager are defined by the Law of Georgia "On Information Security", "On Establishing Minimum Standards for Information Security Managers of the Entities of Critical Information Systems of the First and Second Categories" by the Order of the Head of the Operational-Technical Agency of the State of Georgia of 03 May 2022 No. 12 and the job description, which includes:

- 6.2.1. Daily monitoring of compliance with information security policy requirements;
- 6.2.2. Description of information assets and their access;
- 6.2.3. Coordination of information security management system documentation (policies, instructions, manuals, etc.) draft preparation, approval and review processes;
- 6.2.4. Collecting information about information security incidents and monitoring the response to them;
- 6.2.5. Reporting on information security issues and other administrative/organizational activities;
- 6.2.6. Organizing and conducting general and dedicated information security trainings;
- 6.2.7. Other duties determined by the critical information system entity;
- 6.2.8. Drawing up an action plan and submitting the annual report on the implementation of this plan to the persons and agencies specified in paragraph 2 of Article 2 of the above-mentioned standards;
- 6.2.9. In agreement with the Information Security Board, the admission of the agency's computer incident support team to the organization's network sensor and/or the organization's information asset, information system, or information infrastructure, and notification of the said decision.

7. Third parties

7.1. The third party (including a representative of the contractor organization, an authorized person of the supplier organization), who will have access to the

information assets belonging to the organization and/or will participate in their processing, is obliged to get acquainted with the information security policy of the organization and to comply with the policy regulations.

8. Asset management

8.1. The organization ensures the identification and classification of information assets, as well as establishing rules for their replacement and destruction.
8.2. A responsible person is defined for each identified asset.
8.3. The rules for identifying and classifying information assets are defined in the methodology for identifying and classifying information assets;

9. Risk management

9.1. The information security management system of the organization is based on the information security risk management process, within the process the organization:
9.1.1. determines the approaches to identifying and assessing information security risks;
9.1.2. identify information security risks and analyze their impact and conduct risk analysis;
9.1.3. In order to manage risks, selects the necessary control mechanisms and determines the acceptable risk level;
9.1.4. Prepare a risk management plan.
9.2. Details of the risk management process are provided in the risk identification and assessment methodology.

10. Applicability statement of control mechanisms

10.1. The information security manager will prepare an application for the applicability of control mechanisms, which will contain:
10.1.1. control objectives and control mechanisms selected for information security requirements, as well as justification for their selection;
10.1.2. control objectives and control mechanisms already implemented in the organization;
10.1.3. Rejected (control mechanisms that were not used) list the purpose of controls and control mechanisms, as well as the justification for exclusion.
10.1.4. The organization ensures the achievement of the goals of the control mechanisms, which implies the allocation of efficiency and resources, as well as the definition of the necessary roles and responsibilities.
10.2. To achieve the goals of the information security management system, the organization:
10.2.1. implements selected control mechanisms;
10.2.2. After the introduction of control mechanisms, it observes them;

10.2.3. will analyze the results of the observation and, if necessary, define an action plan.

11. Raising awareness and developing competencies

11.1. The organization will develop and implement information security awareness raising programs, as well as constantly take care of the development of employee competencies.

11.2. Approaches of the organization to raising awareness and development of competencies Organization:

11.2.1. determines the level of knowledge of the employees involved in the dissemination of the information security management system;

11.2.2. will conduct trainings and various activities to meet information security requirements;

11.2.3. maintain records of education, training, skills, experience and competence;

11.2.4. Assess the level of staff knowledge and awareness of the importance of information security measures.

11.2.5. It shows the employees' personal personal responsibility for their own actions or inactions and general obligations to protect the information belonging to the organization;

11.2.6. Make available to employees and point to additional sources of information as well as contact information in all necessary directions.

11.3. Awareness raising programs are planned taking into account the role and obligations of the employee in the organization to ensure knowledge and compliance with information security rules and obligations defined by policies, standards, legislation and agreements.

11.4. Awareness programs should be updated periodically, in accordance with the organization's policies and procedures, at least once a year.

12. Management of information security management system documents

12.1. The organization will ensure the availability of the latest version of the information security management system documentation (in electronic form) to all interested parties, as well as ensure proper protection and control of the management system documentation.

12.2. The organization keeps proper records within the framework of the information security management system, provides their support, protection and control in accordance with the requirements of the management system, detailed information is provided in the document control procedure.

13. Management of information security incidents

13.1. The organization ensures the effective implementation of the information security incident management process, which is led by a computer security specialist;

13.2. All information security incidents are recorded and processed in accordance with established rules.

13.3. The information security incident management process includes the stages of incident identification, response, record collection, resolution, review, and knowledge sharing.

13.4. The organization ensures communication of incidents with interested parties in compliance with the rules established by law.

14. Business continuity management

14.1. The organization will carry out an analysis of the impact of business processes on aspects of information security and, accordingly, will establish continuity plans according to information security requirements, which will allow the organization to restore all necessary services in a short period of time during crisis situations and disasters.

14.2. For the purposes of the information security management system, the organization defines information security continuity criteria, roles and responsibilities, procedures in the event of a major incident, and service availability target indicators.

15. Internal audit of information security management system

15.1. The organization will conduct an audit of the information security management system at the established periodicity and determine the compliance of the system:

15.1.1. With legal and standard requirements;

15.1.2. With information security requirements.

15.2. In order to effectively conduct audits, the organization develops audit programs, criteria and the scope of each audit. Audit programs should take into account the importance of relevant processes and the results of previous audits.

15.3. To perform the audit, the organization will select such auditors and facilitate such an audit process that will meet the requirements of independence and impartiality of the audit process.

15.4. The result of the audit will be submitted to the Information Security Board for consideration.

15.5. To eliminate identified non-conformities, the organization will prepare a plan and ensure effective implementation of the elimination process.

15.6. Documented information about audit programs and audit results will be kept for a period of time agreed with the Information Security Board.

16. Penetration test in the information system

16.1. The organization will periodically conduct penetration testing of information systems aimed at detecting misconfigurations/weaknesses in the systems;

16.2. In order to eliminate the weaknesses identified as a result of testing, the organization will prepare an action plan and ensure the effective implementation of the elimination process.

16.3. A penetration test or vulnerability assessment will be performed as carefully as possible and will be planned, documented and repeatable.

16.4. A penetration test or vulnerability assessment should only be performed by or under the supervision of a competent authorized person.

17. Policy Review Plan

17.1. The information security manager ensures policy updating, continuous improvement and its compliance with the goals and objectives of the organization;

17.2. The policy should be reviewed at least once a year, as well as after significant changes in the organization.

17.3. Policy revisions may also be made in accordance with changes in the business environment, legal and/or technical requirements.

18. Related documents

The information security policy is related to the following documents:

18.1. The scope of information security management system;

18.2. Information Security Board Regulations;

18.3. Organizational context document.