18/7 Henerala Almazova Str., office 408, Kyiv 01133, Ukraine

APPROVED:

Director

Livshyts Vadim Yakovych

Information Security Policy of INTEGRATED REAL ESTATE SERVICES LLC

CONTENT

1. PURPOSE AND GENERAL PROVISIONS
2. REGULATORY REFERENCES
3. TERMS
4. OBJECTS OF PROTECTION
5. BASIC PRINCIPLES AND OBJECTIVES OF INFORMATION SECURITY
6. DISTRIBUTION OF POWERS AND RESPONSIBILITIES
7. REVIEW OF THE DOCUMENT

PURPOSE AND GENERAL PROVISIONS

Information Security Policy (hereinafter - the Policy) defines a set of rules, requirements and guidelines in the field of information security, which are guided by LLC " INTEGRATED REAL ESTATE SERVICES " (IRES) in its activities, as well as defines the basic principles and objectives of information security management (hereinafter - SUIB).

The policy is the normative basis for the protection of information assets of the IRES in order to ensure:

confidentiality - ensuring access to information, information systems and other software processes only for authorized users who have been given the appropriate authority to the minimum extent necessary;

integrity - protection of accuracy, correctness and completeness of information and methods of its processing;

accessibility - means that an authorized user or a process that has the appropriate authority can at any time without much difficulty access the information systems of the IRES ;

- observability - providing the ability to monitor the actions of users, the processes that work with the information assets of the IRES, the time and date of such work, as well as ensuring the principle of impossibility to abandon the actions taken.

1. The policy is based on the requirements of international standards in the field of information security.
2. This Policy is a first level information security document. Level 2 documents are a detail of this Policy in specific areas and on specific issues (Regulations, Rules, Instructions, etc.).
3. This Policy is mandatory for application in the IRES and familiarization with all employees and management of the IRES.

REGULATORY REFERENCES

The policy is developed in accordance with the international standard ISO / IEK 27001 2013 "Information technologies - Methods of protection - Information security management systems - Requirements".

TERMS

For the purpose of equal understanding and proper implementation of this Policy, the terms, definitions, abbreviations, symbols and abbreviations have the following meanings (unless otherwise stated in the text of the Policy):

Information security - protection of information from unauthorized and / or unwanted disclosure (breach of confidentiality), distortion (breach of integrity), loss or reduction of the availability of information, as well as its illegal reproduction.

Information assets - information in any form, information carriers, information systems, telecommunications networks, software in any form of its receipt (purchased or self-developed), which must be protected in accordance with the purpose of information protection.

An authorized user is an employee of the Federal Reserve or a third party who has the authority to use a certain information system of the Group, has registered and is in the system under his unique login.

Threat - actual or potentially possible actions to implement dangerous influencing factors, with the aim of intentional or accidental (unintentional) violation of the functioning of information systems and violation of the properties of protected information or other information assets.

vulnerability - a shortcoming in the information system, program, equipment, the use of which can lead to a violation of the integrity of the system and its incorrect operation. Vulnerabilities arise as a result of programming errors, shortcomings that were allowed during system design, unreliable passwords, malicious programs, etc.

IS risk is the probability that a certain threat can be successfully implemented, which could harm the interests of the IRES.

isolator - a person who has made (tried) to make unauthorized access to system resources (attempt to perform prohibited actions with this resource) by mistake, ignorance or knowingly with malicious intent (for selfish or other reasons) or without such (for self-affirmation, etc.) and used various opportunities, methods and tools.

The Information Security Management System (ISMS) is a part of the general management system of the IRES , based on risk assessment, which creates, implements, operates, monitors, reviews, maintains and improves information security.

IS management is a cyclical process that includes awareness of the need to protect information and setting tasks; collection and analysis of data on the state of information security within the IRES ; IS risk assessment; planning of measures to minimize risks; implementation and implementation of appropriate control mechanisms, distribution of roles and responsibilities, staff training, operational work on the implementation of protective measures; monitoring the functioning of control mechanisms, evaluating their effectiveness and appropriate corrective actions.

OBJECTS OF PROTECTION

The main objects of protection of the information security system in the IRES are:

- territorially distributed information infrastructure, including information processing and analysis systems, hardware and software for its processing, transmission and display, including information exchange and telecommunications channels, information protection systems and facilities, facilities and premises;

- information systems with limited access, as well as open (publicly available) information necessary for the work of the IRES , regardless of the form and type of its provision;
- software and hardware of business processes of the IRES;
- information processing processes in the information system, information technology, regulations and procedures for collecting, processing, storing and transmitting information, staff of developers and users of the system, as well as its staff.

BASIC PRINCIPLES AND OBJECTIVES OF INFORMATION SECURITY

The main purpose of the information security system is to protect corporate information systems of the IRES from possible damage as a result of accidental or intentional impact on information, its media, information processing, storage, transmission, as well as minimizing the risks.

The main objectives of the IS Group support activities are:

- forecasting and timely detection of threats to the security of information assets of the Federal Reserve , the causes and conditions that contribute to harm, disruption of business processes;
- creation of conditions for the functioning of the IRES with the lowest probability of realization of threats to the security of information assets and damage to them;
- identification of potential threats in the field of IS and vulnerabilities of protected objects;
- prevention of incidents in the field of IS;
- creation of mechanisms and conditions for prompt response to threats in the field of IS and manifestations of negative trends in the functioning of information assets of the IRES;
- creation of conditions for the maximum possible compensation and localization of the damage caused as a result of incidents in the field of IS;
- raising awareness of employees of the IRES, and in some cases - and third parties, in the field of risks associated with the use of information assets of the IRES , and their possible consequences.

The construction of the information security management system and its operation should be carried out in accordance with the following basic principles:

- legality (provides for the implementation of protective measures and the development of information security system in accordance with current legislation of Ukraine and international security standards);
- systematic (when creating a security system must take into account all the weaknesses and vulnerabilities of the information system, as well as the nature, possible objects and directions of attacks on it by violators, ways to penetrate distributed systems and unauthorized access to information);
- complexity (integrated use of methods and means of protection of computer systems involves the coordinated use of heterogeneous means in building a holistic system of protection that covers all significant channels of threats);
- continuity of protection (the process of ensuring information security, which should be carried out on a regular basis at all levels within the IRES, with each employee of the IRES must participate in this process);
- timeliness (provides for a precautionary nature of information security measures);
- improvement (involves continuous improvement of measures and means of information protection);
- reasonable sufficiency (assumes compliance of the level of costs for information security with the value of information resources and the amount of possible damage from their disclosure, loss, leakage, destruction and distortion);
- personal responsibility (according to this principle, the division of rights and responsibilities of employees is built in such a way that in the event of any violation, the circle of persons involved in such a violation was clearly known or minimized);
- minimization of authority (access to information should be provided only if and to the extent that it is necessary for the employee to perform his duties);
- flexibility of the protection system (the information security system must be able to respond to changes in the external environment and conditions of the IRES 's activities);
- ease of application of means of protection (mechanisms and methods of protection should be intuitive and easy to use);
- mandatory control (control over the activities of any user, each means of protection and for any object of protection should be carried out on the basis of the use of means of operational control and registration and should cover both unauthorized and authorized actions of users).
- The IRES uses the following requirements to ensure information security:

- periodic inventory of authorized and unauthorized devices in the corporate network;
- periodic inventory of authorized and unauthorized software of servers, workstations;
- use of secure configurations for hardware, network and software, restriction and control of network ports;
- management of software and hardware vulnerabilities, their timely elimination (patch management);
- delimitation and periodic control of users' access rights;
- minimization and control over the use of administrative accounts;
- effective password protection;
- email and web browser protection;
- malware protection;
- constant monitoring and analysis of system logs of audit of work at all levels of information systems;
- protection and control of the use of the corporate network;
- possibility of data recovery;
- cryptographic protection of information.

DISTRIBUTION OF POWERS AND RESPONSIBILITIES

1. The IRES management coordinates the activities of all units to organize information security processes.
2. As part of the implementation of this Policy, information systems are regularly monitored and audited.
3. The head of the IRES is responsible for acquainting employees with the requirements of this Policy.
4. Administrators of information systems ensure the continuous operation of all elements of automated systems and processes, as well as are responsible for the implementation of measures necessary for the implementation of this Policy.
5. Each employee is responsible for compliance with the requirements set out in this Policy, other rules, instructions, recommendations and other internal documents in force within the IRES, as well as for timely notification of direct management of all suspicious situations and possible incidents.
6. Violations of this Policy may be subject to the measures provided by labor legislation.

REVIEW OF THE DOCUMENT

The policy is revised as necessary in the event of the emergence and / or change of information assets of the IRES and / or new technologies, as well as in the event of changes in legislation and other norms and requirements.