

Search

[Electronic in accounting registers](#)
[idol preservation of records](#)
[regulations on the order of provision](#)
[on approval](#)

[APPENDIX](#)
[In the accounting registers](#)
[idol of electronic records](#)
[order of safety](#)
[Regulations on](#)

[Chapter 1. The general rule](#)

[Chapter 2. Idol of electronic records](#)
[to ensure compliance](#)
[organizational measures](#)

[Chapter 3 Idol of electronic records](#)
[maintenance techniques](#)
[measures](#)

[Chapter 4 Final rules](#)

DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN
MINISTRY
SECURITIES MARKET UNDER THE STATE COMPETITION COMMITTEE OF THE REPUBLIC OF UZBEKISTAN
COOPERATION AND DEVELOPMENT CENTER
RESOLUTION

ENSURING THE ESSENCE OF ELECTRONIC RECORDS IN ACCOUNTING REGISTERS
ON APPROVAL OF THE PROCEDURE ON PROCEDURE

[Registered by the Ministry of Justice of the Republic of Uzbekistan on December 11, 2015 No. 2739]

In accordance with the [Law](#) of the Republic of Uzbekistan "On Securities Market", the Republic of Uzbekistan Valuable under the Ministry of Information Technologies and Communications Development and the State Competition Committee The Center for Coordination and Development of the securities market decides:

1. The register of electronic records on the procedure to ensure the safety of [the appendix](#) be approved accordingly.

2. This resolution becomes effective after three months from the date of official publication.

Minister of Information Technologies and Communications H. MIRZAKHIDOV

Tashkent,
November 12, 2015,
139-mh-son

Head of the Center for Coordination and Development of the Securities Market under the State Competition Committee
director B. ATAXANOV

Tashkent,
November 12, 2015,
2015-20

Information of the Republic of Uzbekistan
technologies and communications
Ministry of Development, State Competition
Securities under the Committee
market coordination and development
139-mh of the Center on November 12, 2015,
[Resolution No. 2015-20](#)
APPENDIX

On the procedure for ensuring the integrity of electronic records in accounting registers

NIZOM

This Regulation of the Republic of Uzbekistan " [On Securities Market](#) ", " [Electronic digital signature](#) "and" [electronic document management](#) "in accordance with the laws of the central securities depository, and determines the procedure for ensuring the integrity of electronic records in the accounting registers of the investment intermediary.

Chapter 1. The general rule

1. The following main concepts are used in this Provision:

responsible officer - input, review and modification of electronic records, as well as identity registers, authorized for administrative management of the local network of data transmission, information protection and antivirus support and an employee of the Central Securities Depository or investment intermediary in charge;

electronic record - in the accounting registers of the Central Securities Depository and the investment intermediary electronic recording;

accounting registers - valuable in the investment intermediary and the Central Securities Depository standards of depository operations on storage of securities and accounting of rights to securities record system defined by;

software and hardware - to ensure the integrity of electronic records in the accounting registers To perform the tasks assigned to them by the Central Securities Depository and the investment intermediary a set of hardware and software used;

users of software and hardware (hereinafter referred to as users) - identification officials and other persons exercising the right to use and transfer information in the registers;

influential information - securities resulting from disclosure, modification, destruction or concealment information to be protected from possible harm to market participants;

use of insider information in the securities market - acquisition or sale of securities undisclosed (undistributed) and disclosed (liquidated) securities have a significant impact on changes in value giving preference to one participant in the stock market over another because it can show use of available information.

Chapter 2. Organizational measures to ensure the safekeeping of electronic records

2. Head of the Central Securities Depository and investment intermediary (hereinafter referred to as the head of the investment intermediary) appoints responsible staff and ensures the integrity, confidentiality, integrity and reliability of electronic records take other organizational measures.

3. The manager is obliged to comply with the requirements and rules of work with each responsible employee with information, as well as confidential, effective and disclosure (distribution) may lead to the use of insider information in the stock market a written agreement on liability for the disclosure of other information that is available - an obligation.

4. Central Securities Depository and investment intermediaries basic rules, goals and objectives, protection objects, threats to information security, order of actions in case of violation of information security, division of responsibilities, information approved information security, which provides for the review and updating of security policy must have a policy.

5. Regulate the behavior of officials responsible for the Central Securities Depository and investment intermediaries disruptive, confidential, influential and disclosure (distribution) leading to the use of insider information in the stock market protection and non-disclosure of other types of information that may come in, as well as a threat to information security system of software and hardware complex (hereinafter referred to as the system) in the event of disruptive emergencies approved action plans aimed at speedy recovery and mitigation of the consequences of such situations; should have instructions.

6. Unauthorized use of the manager's accounting registers and the information contained in them from such information ensure the prevention of transmission to persons without the right to use by taking the following measures Required:

defining the scope of users;
accept different levels of usage and allowed functions for each user;
determine the frequency and order of change of user passwords.

7. Leader:
Information security management in accordance with the state standards of the Republic of Uzbekistan;
impact on the technical means of their processing and storage, leading to disruption of the operation of accounting registers not to be shown:

availability of necessary technical means, hardware resources and backup systems;
policy in the field of information security of responsible employees, when there are situations that threaten information security periodic training in the requirements of the guidelines governing the behavior of responsible employees;
continuous monitoring of the level of protection of accounting registers;
uninterrupted operation of the software and hardware during the operating day;
ensure that appropriate action is taken against those who use the system without permission.

Chapter 3 Technical measures to ensure the integrity of electronic records

8. Electronic records are kept in accounting registers using software and hardware.

9. The software and hardware package should provide:
personal electronic digital signature and (or) login and password when using account registers identification, authentication, authorization and registration through;
the ability of users to use credential registers based on their level of use and credentials transfer in accordance with the functions of conducting operations in the registers;
the possibility of organizing the use of accounting registers only in certain automated workplaces;
login and (or) logout, recording the time of each event in the accounting registers automated registration of users on the fact of conducting operations, as well as without permission from the system keeping a log of attempts to use;
timely detection of attempts to unauthorized use of accounting registers and facts of unauthorized use;
blocking the system in case of attempted unauthorized use of the system;
to change the password with a certain periodicity set by the system administrator or at his request send requests to users automatically;
storage of backup copies of accounting registers in encrypted form;
as a result of unauthorized use of accounting registers or as a result of malfunction of the software and hardware complex the ability to quickly restore modified or deleted credentials.

10. Rooms where the server equipment of the software and hardware complex is located with a system of access control to them must be equipped.

11. Account in the Central Securities Depository in order to ensure the integrity of electronic records The following three-tier scheme of receiving registry backups is used:
the first level - the backup is performed by creating a reflection of the credential registers on the main server in real time is increased. This level of backup serves to restore the system automatically and quickly when it malfunctions;
second level - on a replication server, where the backup is located in a separate room, a full copy of the main server carried out in real time;
third level - the backup is performed on a separate server located at least three kilometers from the main server the archive copy of the accounting registers is automatically updated once a day at the end of the operating day. is created.

Each subsequent level of backup is a service to restore system performance in the event of inefficiency of the previous backup level does.

12. At each level of backup, several backups that meet the requirements of the backup scheme of that level server can be created.

13. Additional backup to increase system resilience and reliability levels are allowed.

14. At the discretion of the head in order to study the status of work on the backup of accounting registers an appropriate commission consisting of responsible staff shall be formed.
The composition of the commission, the rights, duties and responsibilities of its members, the order of the study is the decision of the head determined by

15. Commission on a quarterly basis, including when the backup is performed on a separate server located remotely upon arrival, examines the status of backup work and draws up a report based on the results of the study.
The minutes shall be drawn up within two working days after the completion of the study and by all members of the commission will be signed.

In the protocol:
the composition of the commission, the full FIO of its members;
date and place of the statement;
the name, date and number of the document on which the study is based;
the amount of backed up information stored at different levels of backup;
study results;
recommendations to address identified deficiencies should be reflected.

16. Placement of the main server and backup of any level is carried out only in the territory of the Republic of Uzbekistan is increased.

17. The required capacity and backup of the workstations and server equipment of the Central Securities Depository a local uninterruptible power supply with the required autonomous operating time, taking into account the transition time to the power supply must be equipped with sources.
The investment broker's server equipment and workstations required power and not less than 30 minutes must be equipped with local uninterruptible power supplies with autonomous operating time.

18. The Central Securities Depository is the second source of uninterrupted supply of server equipment must have a quick backup in the form of an uninterruptible power supply.

19. Reserve of power supply of the software and hardware complex of the Central Securities Depository small electricity the main power supply input from the station and the backup power supply input from the autonomous backup generator is made available.
The backup generator transmits the power supply within thirty minutes in the event of a power failure from other sources and be provided with a sufficient supply of fuel to keep the generator running for at least one day need

Chapter 4 Final rules

20. Laws on the Integrity, Confidentiality, Integrity and Reliability of Electronic Records by Managers and Officials will be responsible in the manner prescribed by the documents.

21. Persons guilty of violating the requirements of this Regulation shall be liable in the manner prescribed by law.