«Approved»

by the decision of the Supervisory Board
of "Mortgage Refinancing Company of
Uzbekistan" JSC

dated May «11» 2021 y.

INFORMATION SECURITY POLICY
OF JSC
"MORTGAGE REFINANCING COMPANY OF UZBEKISTAN"

Tashkent – 2021

1. General Provisions

1.1. Information is a valuable and vital resource of "Mortgage Refinancing Company of Uzbekistan" JSC (hereinafter - the Company). This Information Security Policy provides for taking necessary measures to protect assets from accidental or intentional alteration, disclosure or destruction, as well as to comply with confidentiality, integrity and availability of information, to ensure the process of automated data processing in the Company.

1.2. Each employee of the Company is responsible for compliance with information security, with the priority task of ensuring the security of all Company assets.

2. Purpose and objective of this Policy

2.1. The purposes of this Policy are:

- preserving the confidentiality of critical information resources;
- ensuring continuity of access to the Company's information resources to support business activities;
- protecting the integrity of business information in order to maintain the Company's ability to provide high quality services and make effective management decisions;
- raising user awareness of the risks associated with the misuse of the Company's information resources;
- determining the degree of responsibility and duties of employees to ensure information security in the Company.

2.2. The heads of the Company's divisions should ensure regular control over compliance with the provisions of this Policy. In addition, a periodic audit of compliance with information security should be organized with subsequent submission of a report on the results of this audit to the management.

3. Scope of this Policy

3.1. The requirements of this Policy apply to all information and information processing resources of the Company.

3.2. Compliance with this Policy is mandatory for all employees.

3.3 Contracts with third parties accessing the Company's information and resources shall stipulate the third party's obligation to comply with the requirements of this Policy.

3.4. The Company owns by right of ownership (including intellectual property rights) all business information and computing resources acquired (received) and put into operation for the purposes of its activities in accordance with applicable law.

3.5. Ownership extends to voice communications using the Company's equipment, licensed and developed software, content of e-mail boxes, paper and electronic documents of all functional units and staff of the Company.

4. Responsibility for information assets

4.1. With respect to all the Company's proprietary information assets, assets under the Company's control, and assets used to gain access to the Company's infrastructure, the responsibility of the appropriate Company employee should be defined.

4.2. Changes in ownership of assets, their distribution, changes in configuration and use outside the Company should be reported to the IT specialist and his/her immediate supervisor.

5. Control of access to information systems

5.1. Rules of work with the Company's information resources

5.1.1. All work within the Company's offices shall be performed in accordance with official job duties only on computers and other devices authorized for use in the Company.

5.1.2. Bringing personal laptops and external storage media (disks, floppy disks, flash cards, etc.) into the Company's buildings and premises, as well as taking them outside the Company, shall be done only with the approval of the General Director of the Company.

5.1.3. All data (confidential or strictly confidential) constituting a trade secret of the Company and stored on hard disks of portable computers shall be encrypted. All portable computers of the Company shall be equipped with hard disk encryption software.

5.1.4. Heads of departments should periodically review the access rights of their employees and other users to relevant information resources.

5.1.5. In order to ensure authorized access to the information resource, any login to the system shall be made using a unique user name and password.

5.1.6. Users shall be guided by recommendations to protect their password at the stage of its selection and subsequent use. Users should not share their password with others or share their account with others, including family members and significant others, if the work is done at home.

5.1.7. Employees are required to always use the password-protected Screen Saver mode during their work. It is recommended to set the maximum idle time of the computer before the screen saver appears to be no longer than 15 minutes.

5.2. Rules of access of third parties to the Company's systems

5.2.1. Each employee must immediately notify the IT specialist and his/her immediate supervisor of all cases of granting third party access to the resources of the corporate network.

5.2.2. Third party access to the Company's information systems must be due to business necessity.

5.3. Rules for granting remote access

5.3.1. Users are granted the right of remote access to the Company's information resources taking into account their relationship with the Company.

5.3.2. Employees who use the Company's portable computers in their work may be granted remote access to the Company's network resources in accordance with their rights in the corporate information system.

5.3.3. Employees working outside the Company using a computer not owned by the Company are prohibited from copying data to the computer from which remote access is provided.

5.3.4. Employees and third parties authorized to remotely access the Company's information resources must comply with the requirement that their computer is not simultaneously connected to the Company's network and to any other networks not owned by the Company.

5.3.5. All computers connected via remote access to the Company's information network must have anti-virus protection software with the latest updates.

5.4. Rules of access to the Internet for employees

5.4.1. Internet access is provided for business purposes only and may not be used for illegal activities.

5.4.2. The rules for the use of the Internet by the Company's employees are as follows:

- use the Internet network for business purposes only;
- it is prohibited to visit any Internet site that is considered offensive to public opinion or contains information of a sexual nature, propaganda of racial hatred, comments on the difference/ superiority of sexes, defamatory statements or other materials with offensive statements about someone's age, sexual orientation, religious or political beliefs, national origin or disability;
- it is prohibited to use the Internet for storing corporate data;
- it is allowed to work with Internet resources only in the mode of viewing information, excluding the possibility of transferring the Company's information to the Internet;;
- it is not allowed to use personal accounts provided by public providers on the Company's equipment;
- check for viruses on files opened or distributed via the Internet;
- access to the Internet via the Company's network is prohibited for all persons who are not Company employees, including family members of Company employees;

- use social network resources in case of emergency for business purposes, and only with the permission of the management.

5.4.3. IT specialist has the right to control the content of the entire flow of information passing through the communication channel to the Internet in both directions.

6. Protection of equipment

6.1. All computer equipment (servers, desktop and laptop computers), peripheral equipment (e.g., printers and scanners), accessories (e.g., mouse manipulators, ballpoint manipulators, CD drives), communications equipment (e.g., fax modems, network adapters and hubs) are collectively referred to as "computer equipment" for purposes of this Policy. Computer equipment provided by the Company is the property of the Company and is intended to be used solely for business purposes.

6.2. Employees must be mindful at all times of the need to ensure the physical security of the equipment on which Company information is stored.

6.3. It is forbidden to change the configuration of hardware and software on their own. All changes are to be made by an IT specialist after the changes have been agreed upon with his/her immediate supervisor.

6.4. Users of portable computers containing the Company's trade secret information must ensure their storage in physically protected rooms, locked desk drawers, cabinets, or protect them with a similarly effective protective device when the computer is not in use.

6.5. Every employee who has been given a laptop computer is obliged to take appropriate measures to ensure its safety, both in the office and at their place of residence. In situations where there is an increased risk of theft of laptops, such as hotels, airports, offices of business partners, etc., users are obliged not to leave them unattended under any circumstances.

6.6. The laptop computer should be kept in the trunk when traveling in a car. It should be moved from the vehicle to the hotel room overnight.

6.7. All computers should be password protected at system boot, hotkey activation and after exiting the "Screen saver" mode. The user must contact technical support to set the protection modes. Data must not be compromised in the event of negligence or carelessness resulting in loss of equipment. All equipment components that include data media (including hard drives) must be inspected prior to disposal to ensure that they are free of sensitive data and licensed products. A procedure for formatting storage media must be followed to ensure that data cannot be recovered.

6.8. When writing any information to a storage medium for transferring it to counterparties or business partners, it must be ensured that the medium is clean, i.e. does not contain any other data. Simply reformatting the medium does not guarantee the complete deletion of the information recorded on it.

6.9. Pocket PCs, as well as cell phones with e-mail function and other portable devices are not among the devices with reliable data protection mechanisms. It is not recommended to store confidential information in such a device.

6.10. Data transfer ports, including FD and CD drives in stationary computers of the Company's employees are blocked, unless the employee has received permission to record information from the Company's management.

7. Software protection

7.1. All software installed on Company-provided computer equipment is the property of the Company and must be used solely for business purposes.

7.2. Employees are prohibited from installing non-standard, unlicensed software or software unrelated to their work activities on the computer equipment provided for use. If unauthorized software is discovered during maintenance, it will be removed and a report of the violation will be made to the employee's immediate supervisor and the Company's General Manager.

7.3. All laptop computers must have installed on them the programs necessary to provide information security:

- personal firewall;
- anti-virus software;
- hard disk encryption software;
- mail encryption software.

7.4. All computers connected to the corporate network shall be equipped with an anti-virus protection system approved by the IT-specialist and his/her immediate supervisor.

7.5. Company employees shall not:

- block antivirus software;
- install other anti-virus software;
- change settings and configuration of antivirus software.

7.6. The Company prefers to purchase software rather than develop its own programs, so users wishing to implement new software or improve existing software should discuss their proposal with their immediate supervisor.

7.7. The head of the initiating unit should discuss the introduction of new software or improvement of existing software with the IT specialist and his/her immediate supervisor, and then with the Company's management.

7.8. If general approval is given for the introduction of new software or enhancement of existing software or the purchase of external devices, the Company shall take appropriate action in accordance with the established rules for procurement procedures.

8. Rules for the use of e-mail

8.1. Electronic communications (whether deleted or not) may be accessed or obtained by government agencies or business competitors for use as evidence in legal proceedings or in the conduct of business. Therefore, the content of electronic communications must strictly comply with corporate standards for business ethics.

8.2. Employees are prohibited from sending the Company's confidential information to partners via e-mail without the use of encryption systems. Strictly confidential information of the Company shall under no circumstances be forwarded to third parties via e-mail.

8.3. Employees of the Company are prohibited to use public e-mail accounts for any of the corporate activities.

8.4. The use of public e-mail accounts by the Company's employees is carried out only with the approval of the IT-specialist and his/her direct supervisor, provided that encryption mechanisms are used.

8.5. Company employees should use only their official e-mail address to exchange documents with business partners.

8.6. E-mail messages are a permanently used tool for electronic communications with the same status as letters and faxes. Electronic messages are subject to the same approval and retention as other means of written communication.

8.7. To prevent errors in sending messages, users should carefully check that the names and addresses of recipients are spelled correctly before sending. If a message is sent to an incorrect address, the IT specialist and his/her immediate supervisor should be informed immediately.

8.8. The sender of an electronic message, document or the person who forwards it should indicate his/her name and surname, business address and the subject of the message.

8.9. The following are unacceptable behaviors and uses of e-mail:

- sending messages of a personal nature that utilize significant e-mail resources;
- ending messages/emails of a non-work-related nature to all Company users in groups;
- sending promotional materials not related to the Company's activities;
- subscription to mailing lists, participation in discussions and similar services;
- searching and reading messages sent to others (regardless of how they are stored);
- forwarding any materials, both messages and attachments, the content of which is unlawful, obscene, malicious, abusive, threatening, defamatory, malicious or encourages behavior that could be considered a criminal offense or administrative

misconduct, or results in civil liability, disorderly conduct or contravenes corporate ethical standards.

8.10. The user shall add a privacy notice to all outgoing messages sent to external users.

8.11. Attachments sent with messages should be used with due care. Attachments should always include the date they were prepared and should be filed in accordance with the Company's document management procedures.

8.12. Sending significant amounts of data in a single message may adversely affect the overall level of availability of the Company's network infrastructure to other users. The volume of attachments shall not exceed 5 Mbytes.

9. Reporting information security incidents, emergencies and response procedures

9.1. All users should be aware of their obligation to report known or suspected information security breaches, emergencies, and should be informed that under no circumstances should they attempt to exploit known security weaknesses.

9.2. B If a laptop computer is stolen, the incident should be reported immediately to the IT specialist and his/her immediate supervisor.

9.3. Users should know how to report known or suspected information security incidents using telephone, e-mail and other methods. Incident reports should be monitored, recorded and acted upon.

9.4. If the presence of viruses or other destructive computer code is suspected or detected, immediately upon discovery, a member of staff must:

- inform the IT Specialist;
- not use or turn off the infected computer;
- not connect this computer to the Company's computer network until the detected virus has been removed and a full anti-virus scan has been performed by the IT specialist.

9.5. An emergency situation (incident) related to a breach of information security may be caused by:

- destructive impact on the entire property complex of the enterprise in the event of natural factors (flood, fire, earthquake, etc.) or a targeted attack (bombing, arson, destruction of buildings and premises, etc.)
- negative impact exclusively on the information resources of the enterprise (as a rule, carried out remotely, using telecommunication channels).

9.6. Organizational procedures (regulations) for responding to emergency situations:

- Organization of alternative information processing processes (including, possibly, without the use of automation tools) for the period of failure of the main information resources;
- coordination by heads of structural units of personnel actions in case of emergency;
- organization of technical and organizational documentation required to restore information systems and data after an emergency;
- organization of archival (backup) copies of data and software applications of data processing in places protected from mechanical impact, theft, floods, fires, etc. (including, possibly, in locations geographically remote from the main data storage and processing locations);
- agreements with suppliers of software and hardware components included in the enterprise information infrastructure for urgent delivery of components that have failed and require replacement in case of emergency.

10. Premises with technical means of information security

10.1. Confidential meetings (sessions) shall be held only in premises protected by technical means of information security.

10.2. The Company's Conference Hall is a room with technical means of information security.

10.3. Participants of meetings are prohibited to enter the premises with audio/video recording equipment, cameras, radio telephones and cell phones without prior approval of the IT-specialist and his/her direct supervisor.

10.4. Audio/video recording, photographing during confidential meetings may be conducted only by the Company's employee who is responsible for the preparation of the meeting, after obtaining written permission from the head of the meeting organization group.

10.5. Access of participants of a confidential meeting to the room for its holding is carried out on the basis of the approved list, control over which is conducted by the person responsible for the organization of the meeting.

11. Network management

11.1. The IT specialist and his/her immediate supervisor control the content of all data flows through the Company's network.

11.2. Employees of the Company are prohibited to:

- disrupt the information security and operation of the Company's network;
- scan ports or security system;

- monitor the operation of the network with data interception;
- access a computer, network or account bypassing the user identification or security system;
- use any programs, scripts, commands, or transmit messages to interfere with or disable a user of a terminal device;
- transmit employee information or lists of Company employees to unauthorized persons;
- create, update or distribute computer viruses and other destructive software.

12. Data protection and security

12.1. The users are responsible for the security of data on stationary and portable personal computers. The IT specialist is obliged to assist users in backing up data to appropriate media.

12.2. Regular backups of basic service information and software should be made.

12.3. Only the IT specialist can create and delete shared network resources and public folders based on requests from department heads, as well as manage access authorizations to them.

12.4. Employees are authorized to create, modify and delete files and directories in shared network resources only in those areas that are assigned to them personally, to their work groups or to which they have authorized access.

12.5. All requests for computer maintenance should be directed to the IT Specialist.

13. Final Provisions

13.1. All operating procedures and procedures for making changes to information systems and services must be documented, coordinated with the IT specialist and his/her immediate supervisor.

13.2. All employees of the Company shall comply with the requirements of this Policy and shall be liable for non-compliance in accordance with the law.

13.3. Any changes and additions to this Policy are valid if they are made in writing and approved in accordance with the established procedure.