BenchMark
est. 2003

RULES ABOUT INFORMATION SECURITY
OF PERSONAL DATA

I. General terms

These rules are adopted in order to protect and control the computer and information systems of the investment intermediary, as well as to ensure the protection of data and customer information stored with the investment intermediary. The rules are aimed at maintaining reliable systems and networks, ensuring a high level of security, providing access according to the position and function of the loan, performing constant control and timely updating of the software products used.

The operation, protection and control of information and computer systems is performed in compliance with the following basic principles:

1. separation of user from administrator functions;
2. establishing levels and access to information;
3. registration of access, entry, change and deletion of data and information;
4. the implementation of control by specialized units and employees of the intermediary.

II. Maintenance and protection of information and computer systems

The investment intermediary has an independent Information Technology Department (IT Department), whose main functions are the following:

1. Prepares and installs the necessary computer systems (hardware) and software;
2. Provides methodological assistance to employees in their work with computer systems and software;
3. Evaluates and approves the used software and hardware, including the selection of Internet and information service providers;
4. Develops, implements and maintains systems for obstruction and control of unregulated access to information and databases;
5. Implements and maintains antivirus software;
6. Develops, implements and maintains systems for authorization and identification when entering and leaving computer systems;
7. Develops an emergency action plan to preserve computer and information systems and to restore their normal functioning.

III. Rights and obligations of the employees of the investment intermediary with regard to the information and computer systems

The persons working under a contract with the Investment Intermediary are obliged to observe the following general rules when working with computer and information systems:

1. The employee has the right to work on an office computer, as the access to the stored data is carried out by him by entering a username and password;
2. It is prohibited to provide third parties with the personal username and password to log in to the office computer;

3. At the end of the working day, each employee must turn off the computer on which he works or put it in log off mode;
4. In case of loss of data or information from the office computer, the employee shall immediately notify the System Administrator, who shall provide him with appropriate technical assistance;
5. Attempts to access computer information and databases to which no rights have been granted in accordance with the position held by the employee, as well as the performance of any actions that facilitate third parties for unauthorized access are prohibited;
6. The installation and use of illegal software is prohibited.
7. The export of hardware or media containing personal data is prohibited.
8. Employees have the right to exchange computer information through an internal computer network only in connection with the performance of their official duties and only with employees with whom they have direct official relations.
9. Archived computer information is provided only to employees who have the right of access, according to the position they hold and the task performed, in compliance with the principle of "need to know."
10. Access to computer information, databases and software is restricted by technical methods - user identification, passwords, timekeeping, copying bans, tracking of unauthorized access.
11. Specific measures have been introduced to protect information and computer systems against computer viruses, failure of local networks, power outages, etc., as follows:

IV. Protection against computer viruses and other malware

The following measures are applied for anti-virus protection:

1. All personal computers have real-time antivirus software installed, which is updated daily.
2. The system administrator performs the following activities:

   2.1. activates the protection of the respective resources - file system, e-mail and performs an initial full scan of the system;

   2.2. sets up antivirus software for periodic scans over a period of time, but at least once a week.

   2.3. activates the protection of various software products for warning in the presence of macros and adjusts the firewall of the system;

   2.4. checks for properly configured software to automatically update the operating system and installed software;

3. When a message from the anti-virus program for a virus in the local network appears, each employee from the respective workplace must inform the System Administrator.

V. Business continuity

<u>The following measures are applied in case of local network failure:</u>

1. All personal computers are connected to an uninterruptible power supply.
2. In the event of a power failure, all employees are required to immediately save all files they have opened on the servers and stop working.
3. In the absence of power for more than 10 minutes, the System Administrator begins a procedure for phasing out the servers.
4. In the event of a failure on the local computer network, each user should save the files he has opened on his local computer to avoid losing information. When restoring the network, all locally saved files should be moved back to the server and the local copies deleted.

VI. Backup

<u>Information, including that containing personal data, shall be backed up as follows:</u>

1. Automated and scheduled backup of all operating information on servers and disk arrays.
2. Data backup is performed in a way that allows, if necessary, the data to be installed on another server / computer and to continue the work process without significant data loss;
3. Eurosys System databases are backed up every night;
4. Shared documents are backed up twice a week.

VII. Access control and rules for working with media

<u>The following measures for secure entry into the system are applied:</u>

1. Each employee has specific access rights and uses a unique user ID to log in and access the directory to which he is authorized so that he can be identified. The use of group IDs is not allowed;
2. Control of the management and protection of access to network connections and network services is performed by means of an active directory with a specific username provided by the System Administrator, which controls the computers used to access networks and network services.
3. The provision of access is done according to a defined internal company order, setting certain rights of access to specific information resources, according to the loan position and function. No unauthorized persons are assigned or provided access.
4. The system administrator shall immediately revoke the access rights of persons who are no longer employees;

5. The system administrator performs an ongoing check to remove or block redundant IDs and accounts and does not provide redundant user IDs to other users;
6. Data processors use unique passwords of sufficient complexity that are not recorded or stored online;
7. All system-level access passwords are changed periodically;
8. Emails containing sensitive information or personal data are sent via an encrypted connection.
9. All personal data carriers are stored in a safe and secure environment - in accordance with the specifications of the manufacturers, in locked cabinets, with limited and controlled access.
10. When transporting media outside the physical boundaries of the company's office, they are placed in appropriate packaging and in a sealed envelope. Employees are strictly prohibited from using mobile computing devices in places where there may be a risk to the device and the information in it. Users of mobile computing devices and mobile phones are responsible for protecting them from theft and do not leave them unattended.
11. Employees are required to avoid any risk of access to information by unauthorized persons as well as malicious software. Disclosure of confidential and sensitive information by mobile phones in places where it may become available to third parties is prohibited.
12. Once no longer needed, media is destroyed safely and securely to reduce the risk of leaking sensitive information to unauthorized persons. The physical destruction of the information media is by breaking it. They are checked in advance to make sure that the necessary information is copied and then all the information is deleted from them before destruction.

VIII. Final provisions

This policy is reviewed and evaluated periodically for its effectiveness, and the investment firm may adopt and implement additional measures and procedures that are appropriate and necessary to protect the information.

This policy is made available to employees for information and execution, and the Board of Directors may issue orders and instructions regarding its implementation.