INFORMATION SECURITY REQUIREMENTS

For mitigation of risks of unauthorized access to Customer's accounts by violators and key information compromise, Bank earnestly asks Customers to follow the next information security measures.

- To dedicate a computer which will not be used for any other purposes except for working in System; not to perform Internet access from this computer, and if it's technically feasible to forbid it, on Internet addresses different from Bank's servers addresses.
- To limit or completely forbid remote access to dedicated computer from other local network computers. Not to use remote administration tools on dedicated computer. If it is technically feasible, to put dedicated computer in separate network controlled with network firewall and intrusion detection systems.
- To replace all standard passwords set on System installation with unique personal ones, to implement periodical passwords alternation (not less than once in three months).
- To constantly use an anti-virus software with updated databases.
- To implement on a regular basis (not less than once a week) anti-virus check for timely detection of malicious software.
- To use only licensed software on computer.
- To perform operating system updates on a regular basis (not less than once a month or upon publication of updates).
- To check "Administrators" group on dedicated computer, to exclude basic users, which don't work with System, from this group.
- If it is technically feasible, create separate group policy for users working with System, which allows start-up of only specified programs.
- To use only foreknown Internet addresses of servers for Bank's servers access.
- To instantly inform the Bank in case of Bank's server connection unavailability.
- To store in safe place (safety cabinet) and not to hand anyone key data storage devices, to assure access to them only by authorized persons.
- Never implement copying of private (secret) keys of electronic signature on local hard drive, even with following deletion.
- Timely (accordingly to terms of Agreement) implement the scheduled working keys change.
- On a regular basis (not less than once a month) check Key storage devices integrity by implementing check of electronic signature files presence.
- Not to leave key data storage devices unattended, connect them with computer only for usage time and instantly disconnect them after banking operations implementation. Always lock display by entering password when leaving place of work with System unattended.
- To perform instant electronic signature key change in case of its compromise or assumption of compromise.
- Timely install all System's updates.

- Not to install updates and not to open links in e-mail messages received from Bank's name, not to open links in such e-mails, inform the Bank instantly of such received messages.

- Implement additional log in to System for outcoming messages control on a daily basis during Bank transaction day and after working day to. In case of suspicious documents detection, instantly address to Bank.

- In case of assumption of computer work slowdown, cut it off from local network and Internet physically and refer to system administrator with request for necessity of full ant-virus check implementing by scanning all files in computer's memory.

- In case if information security incident has anyway happened, never power off computer, only physically cut it off from local network and Internet, instantly refer to system administrator and report incident to Bank for carrying on-the-spot investigation and for taking necessary means for evidences gathering.

- In case of recognition of suspicious operations in System by Customer instantly report it to Bank.