Instruction of System Safe Use

1. Setting up your PC

- The system login should be conducted from secure computers only with installed antivirus software.
- When you enter the system please make sure that the real address (link) of the Raiffeisen Online System is specified in the link field of the web-browser: https://online.aval.ua.
- When you log into the system please check that encryption is on. If the encryption is on the following image will appear in the web-browser window.
- There should be a confirmation that a secure connection is set up between the user's web-browser and the Bank's web-server. A digital (electronic) certificate of the Bank server for this purpose. It's important to check the security of the certificate's provider, certificate validity and its validity term.

The digital certificate of the Bank is reliable

- ✓ **Issued online.aval.ua**
- ✓ **Expires from 29.08.2017 to 28.11.2020**

- The PC used for system entry should have:
  1. a regularly updated operational system;
  2. an installed latest version of supported web-browser;
  3. security software containing a licensed antivirus software, antispyware and firewall or brandmouse*.
- It is recommended to activate the function of automatic operational system update on PCs with Windows OS.
- Antivirus databases and antispyware should be regularly updated.
- We recommend you to conduct full scanning of the workstation regularly (not less than once a week) in order to detect viruses and malicious software.
- We don't recommend to install to your workstation software from unreliable resources (public software libraries, software received via e-mails etc.).

2. Password policy

- When you enter the login and password please make sure that nobody is watching you.
- Before changing the password please check the security certificate of the Bank's server
- Don't use the function of password saving which will be proposed by the web-browser.

- • The login must be at least 5 and not more than 30 characters and consist of letters of the Latin alphabet and / or numbers and / or special characters available for entering one of the keys of the standard keyboard of the user of the personal computer.

  The password must meet the following requirements:
  - a minimum of 8 characters;
  - no more than 20;
  - at least 1 small letter;
  - at least 1 large letter;
  - at least 1 digit;
  - at least 1 special character, such as% @,?, *?, and the like;
  - 4-last Passwords for the entry must not coincide;
  - the password for the login is 90 days..

3. General security rules for Raiffeisen Online System usage

- After you've started your session please check the date of last visit to the system and track your activity history in the Raiffeisen Online System using the «My activities» menu.
- If you've conducted login to the System please don't leave your workstation without control.
- The session should be finished by using Logout button and closing the web-browser window.
- If you conduct system login in public workstations it is recommended to clean the browser's cash and delete all temporary files and cookies before the browser window is closed.
- Don't review other websites in the same web-browser when using the Raiffeisein Online Sytem site.
- Please track the web-session duration which is limited to 10 minutes for security reasons.
- Please use the navigation links and buttons of Raiffeisen Online System only and don't use the web-browser's navigation buttons (i.e. Back/Ahead, Refresh etc.)
- Pay attention to the web-browser's notifications about threats.

4. Potential threats

- Don't use system login links via banner links or links received in e-mails.
- Don't reply to requests (mostly sent per e-mails) which contain requirement to provide or check your login, password, secret code (PIN) etc.

  Attention!!! The Bank never sends e-mails with requests to send password, login or go to the link provided in the e-mail.

- The Bank doesn't distribute the computer software via e-mails.
- It is recommended to delete e-mails without opening, especially received from unknown senders, with *.exe, *.pif, *.vbs and other files attached.
- If any malicious software is detected on your workstation (viruses, troyans etc.), please conduct login to Raiffeisen Online System from guaranteed secure workstation and change your password to the System.

5. Detecting problems the their solutions

- If you detect an attempt of unauthorized access to Raiffeisen Online System you should necessarily change the access password and contact the Bank's Call Center to get recommendations for further actions. It's also recommended to conduct scanning of your workstation for detecting viruses and other malicious software.
- If you've lost your customer identification card you should contact the Bank's Call Centre and order the Internet Banking channel blocking. Please visit any branch outlet of the Bank in order to get the new CIN card.

* There's a range of software solutions on the market combining functions of antivirus, firewall, antispyware and other software means for workstation protection